IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme

Mrs. Nagamani K[1], Bhange Yogita[2], Bhoir Dhanashree[3], Dalavi Rani[4]

Professor, SSJCOE, Dombivali (E)[1]

B.E Comp, SSJCOE, Dombivali (E)[2,3,4]

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: Android, Attendance management, E-learning, SMS etc.

I. INTRODUCTION

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the code match, the process will be completed and the user will be authorized for access. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Now day's graphical passwords are other alternatives. The passwords require the following fundamentally requirements so that the problems with passwords arises.

(a) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.

(b) Passwords should be secure, i.e. they should be different and should be difficult to guess.

II. LITERATURE SURVEY

Sobrado proposed three shoulder surfing resistant schemes, triangle scheme, movable frame, and intersection scheme. In triangle scheme,as shown in fig.2.1 the system will randomly distribute 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 as to click inside the invisible triangle created by those objects.[4]

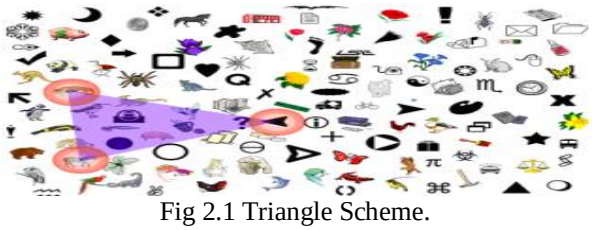

Fig 2.1 Triangle Scheme.

The same concept is used in movable frame. Only the difference is one object from the pass object is given on frame. The pass objects are placed randomly within the frame as shown in fig. 2.2

Fig 2.2. Movable Frame Scheme.

In intersection method this concept has made more complex. It uses two invisible lines and increased the number of pass object as shown in fig.2.3. User have to click on the intersection of two invisible lines, inside the convex quadrilateral formed by those objects.

Fig 2.3 Intersection Method.

Both the interaction and movable frame have high failure rate. In triangle scheme user has to memorize the pass objects and choose those objects.

So the memory burden of the user is high.

T. Yamamoto proposed a shoulder-surfing-resistant image-based authentication system with temporal indirect

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

image selection scheme which consist TIIBA. Although image-based user authentication systems have gotten a lot of attention recently to reduce the burden of memorizing passwords, they can be vulnerable to shoulder-surfing attacks. To overcome this problem, shoulder-surfing-resistant image-based authentications with indirect image selection (indirect image-based authentication, or I-IBA) have been proposed. Therefore, by temporally arranging the image-sets, we implemented another indirect image-based authentication scheme (temporal I-IBA, or TI-IBA) that is not constrained by the screen size and makes it easy for authorized users to recognize their pass-images. 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[7].

So H. Gao et al. proposed graphical password scheme using color login. In this color login uses background color which decrease login time. Possibility of accidential 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. During login phase four pairs of colors and 8*8 matrix will be displayed. As the rating given by the user, the password will be generated. The user has to memorize the rating and order of the colors. So it becomes very hectic to user [2].

Login Interface Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords system is proposed by M.K.Rao et al. In PPC some rules are defined and those are followed by the user to get the session password. But this scheme is very complex and hectic [5].

III. ARCHITECTURE OF PROPOSED SYSTEM

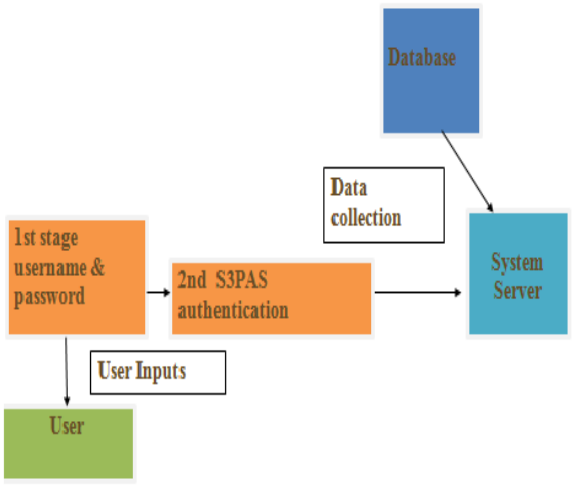

Fig 3.1.Architecture

IV. PROPOSED SYSTEM

This proposed system is being designed to an improved text-based shoulder surfing resistant graphical password scheme by using colors. 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. It will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors. The alphabet used in the propose scheme contains 72 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and 10 symbols that is ".", "/", "@", "#", "$", "%", "&", "*", "?", and "=". The System will work in following steps:

Step 1: Password Registration-In the proposed scheme user has to set textual password K of length L. The minimum length of Password is 8 Characters and the maximum length of password is 15 characters i.e password length is between 8 to 15 Characters, and choose one color as his pass color from 8 colors assigned by the system. And, the user has to register an e-mail address for re-enabling his account when he enters a wrong password. In this scheme, registration process should carried out in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS or any other secure transmission mechanism. The system stores the user's textual password in the users entry in the password table, which should be encrypted by the system key. So in short in registration phase the user set is textual password and select 1 Colour from 8 Colours.

Step 2: Login- In the login phase when an user sends an login request to the system, the system displays a circle which is composed of 8 sectors of equal Size. The colors of the arcs of each sectors is different, and every sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. In this Step 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "counter clockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel.The login screen of the proposed scheme can be illustrated by an example shown in Figure. To login the system, the user has to finish the following steps:

Step 1: The Login Screen is shown to user.

Step 2: After the display of login Screen, The System displays a Circle Composed of 9 sectors of equal size and each sector contain 72 characters randomly and averagely distributed among the sectors. The 72 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the 10 symbols that is ".", "/", "@", "#", "$", "%", "&", "*", "?", and "="are in regular typeface, and the 10 decimal digits are in italic typeface. Again there is a button for rotating the circle clockwise, the button for rotating the Circle anti clockwise, the "Confirm" Fig.3. Flow Chart Of Login Process button, and the "Login" button are also displayed

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

on the login screen. All the characters in sectors are rotated clockwise and anticlockwise by pressing the button clockwise and anticlockwise. The mouse wheel can also be used to move the characters from one sector to another sector. Suppose that, at the start of login session we assume one variable i , and Let i = 1.

Step 3: After step to, in step 3 user has to rotate the sector which contains the Characters of password,and has to move that character in the sector whose color is selected by user, for that purpose many rotate clockwise or anticlockwise operation are performed. After the rotation and click on the confirm button, and after the confirmation increase the value of i by 1.

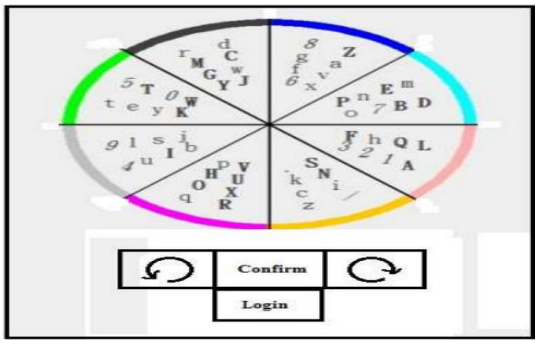

Fig 4.1. Login Screen.

Step 4: If the value of I is less than L, where L is the length of password, then perform step 3 repeatedly until the value of i becomes L , After that click on Login Button and then login process gets complete. To provide the security the user can enters the wrong password only 3 Consecutive times, If the account is not successfully authenticated for three consecutive times, this account will be disabled and the system send the link to the registered email address which can be used by authorized and correct persons to login and re-enable the disabled account.

V. RESULT (SCREEN SHOTS)

S3PASS Authentication Phase

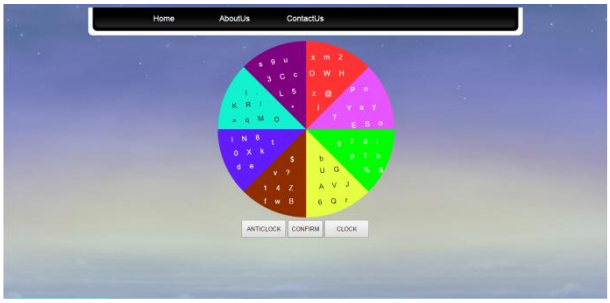

Fig 5.1. S3PASS Authentication phase.

Password received on user mail, the user requests to validate the login into the system. Validation phase of the system displays a circle composed of 8 equally sized sectors. The colours of the arcs of the 8 sectors are different, and each sector is identified by the colour of its arc, e.g., the red sector is the sector of red arc. Initially, 72 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "counter clockwise" button.After selecting each letter of password in that colored arc which user has chosen, he/she have to confirm validation by clicking on "Confirm" button. The validation screen of the proposed scheme is shown in above figure.

OTP Verification Phase

Fig 5.2. Verification phase.

After successful validation phase, another OTP is generated. This OTP send as text message on user's registered mobile number. This OTP verify in this phase for secure login into system. This process shown in above figure.

VI. CONCLUSION

We have proposed a simple text-based shoulder surfing resistant graphical password, in which 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 .Finally, we have analysed the resistances of the proposed scheme to shoulder surfing and accidental login**.**

VII. HARDWARE REQUIREMENTS

- Processor: Core 2 duo
- RAM: 1GB or Higher
- Hard disk: 80 GB or Higher

VIII. SOFTWARE REQUIREMENTS

- Apache Tomcat Server
- Windows Operating System
- Eclipse
- FRONTEND: Java(Jsp/Servlet)
- BACKEND: MySql

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

REFERENCES

[1]. B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.

[2] 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, Dec. 2009, pp. 675-678.

[3] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-47.

[4] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005. and "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[5] M.K..Rao proposed "Login Interface Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords system".

[6] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," Proc. of the 2003 Int. Conf. on Security and Management, June 2003, pp. 105- 111 .

[7] T. Perkovic, M. Cagalj, and N. Rakic, "SSSL: shoulder surfing safe login," Proc. of the 17th Int. Conf. on Software, Telecommunications & Computer Networks, Sept. 2009, pp. 270-275.

[7] 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, July 2009, pp. 188- 194.

[8] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," Proc. of the First Int. Workshop. on Education Technology and Computer Science, Mar. 2009, pp. 90-95.