User Authentication Scheme using Session Passwords Based on Color and Numerical Matrix

Sanidhya Tandon[1] Raghvendra Singh[2] Shubham Sonkar[3] Swasti Singhal[4]
[4]Assistant Professor
[1,2,3,4]Department of Information Technology
[1,2,3,4]Galgotias College of Engineering and Technology, Greater Noida, India

Abstract— User authentication is one of the principal topics in information security. Traditional strong password schemes could provide with certain degree of security; however, strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. As a result, security becomes greatly weakened. Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as an alternative technique to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Multiple colors or images are used to confuse the peepers, while not burdening the legitimate users. Meanwhile, the scheme is resistant to shoulder surfing and intersection attack to a certain extent. Session passwords can be used only once and every time a new password is generated. In this paper, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

Key words: User Authentication; Session Passwords; Shoulder Surfing

I. INTRODUCTION

The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. However, concerning about losing its users' privacy through biometric authentication and high cost of these devices has prevented these techniques from being widely accepted. Strong password authentication is the most widely used authentication method for remote user authentication in network at present. However, most users still prefer their password created from relevant information that they are either familiar with or easy to remember, even its security might not be good enough. Graphical password is a promising solution to this problem . Psychologists have shown that in both recognition and recall tasks, images are more memorable than words or sentences. Various graphical password schemes have been demonstrated as feasible alternatives to alphanumeric-based or biometric-based authentications. But picture-based password schemes still have some drawbacks: The password might be easily guessed when there exits too few or too obvious characteristics in the picture; Many passwords might be identical if the pictures are homogeneous; Like text passwords, the adversaries can view the user's input process by shoulder surfing, and try to impersonate the user later on; The password images, such as created by random art, might be too meaningless to have their users to login to a phishing website without even noticing. In this paper, two new authentication schemes are proposed. These schemes authenticate the user by session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed authentication schemes use text and colors for generating session passwords. The major disadvantage in most of the existing graphical password schemes is that the mouse-click. ColorLogin does depend on mouse clicks, however it is effective in overcoming this weakness. It is possible in ColorLogin that users can click on deceptive icons instead of pass-icons (used as password). Such action makes ColorLogin resistant to shoulder surfing.

II. RELATED WORK

Graphical password schemes based on choosing multiple images as pass objects usually require users to recognize the pre-selected pictures and repeat the correct select actions. As the first choice of multiple images as pass objects scheme, based on Hash Visualization technique [9], Déjà Vu authenticates a user through his ability to recognize previously registered images [5].. Real User employs facial photographs in its graphical password system. Passface [2] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in figure 2. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times. Blonder [5] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Jermyn, et al. proposed a new technique called "Draw- a-Secret" (DAS) where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing. Blonder designed a graphical password

scheme where the user must click on the approximate areas of pre-defined locations. Passlogix extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity. Haichang et al proposed a new shoulder-surfing resistant where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user. Weinshall and Kirkpatrick proposed several authentication schemes such as picture recognition, object recognition and pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes. Goldberg designed a technique known as "passdoodle". This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen. The above-mentioned graphical password schemes have not provided a satisfactory answer for usability and security, the two of major design and implementation issues of graphical passwords.

III. PROPOSED SCHEME

Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

A. Pair-Based Authentication Scheme

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.

Fig. 1: Login Interface

Figure 1 shows the login interface. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits.

Fig. 2: Intersection letter for the pair AN

The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Fig 2 shows that L is the intersection symbol for the pair "AN". The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system. The grid size can be increased to include special characters in the password.

B. The Colour Login Scheme

In Colour Login, the system challenges a user who wants to be authenticated. The challenge is conducted in R rounds and each round provides random icons displayed on the screen. An example of a challenge round is shown in Figure 1; in which red is the focused color while blue and green are inducing ones. A pass-icon is chosen correctly when the user clicks on the row which contains the pass-icon. The icons in that row are all replaced by a substituted Lock icon to resist shoulder-surfing. A round is considered to be a successful one when all the h hiding pass-icons are correctly chosen. In order to reduce users' memory burden, it is not necessary for users to choose in a particular order.

C. Hybrid Textual Authentication Scheme

During registration, user should rate colors as shown in figure 3. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 10. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

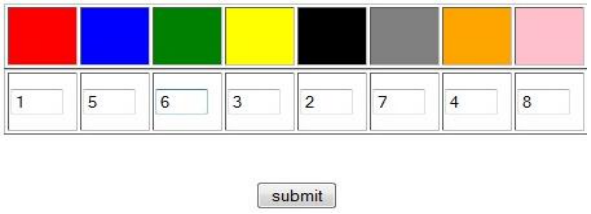

Fig. 9: Rating of colors by the user

IV. PERFORMANCE EVALUATION

A. Resistance to Shoulder Surfing

In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains hidden so the session password can't be enough to find secret pass in one session. ColorLogin provides a shoulder surfing resistant scheme which can overcome the drawbacks noted above. In ColorLogin, there are different icons on the screen in each login round. Neither the icons nor the pass-icons displayed are fixed. When the user finds one pass-icon, he only needs to click on the line where the pass- icon lies, rather than the pass- icon itself. After the action of the mouse, the icons in the clicked line would be replaced by substituted icons. In hybrid textual scheme, the randomized colors hide the password. In this scheme, the ratings decide the session password. But with session password you can't find the ratings of colors. Even by knowing session password, the complexity is 84 .So these are resistant to shoulder surfing.

Dictionary Attack: These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

Guessing: Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 364.The hybrid textual scheme is dependent on user selection of the colors and the ratings. If the general order is followed for the colors by the user, then there is a possibility of breaking the system.

B. Social-Engineering Attacks

Social engineering attacks make use of the possibility that people will give away their information through social telephoning, conversation, or email. In the password images of our scheme, the tracks can be made quite complicate and the number of objects appeared in each segment of the track is varying. Thus, it is not easy to describe in words the locations of the objects of choice.

V. CONCLUSION

In this paper, three authentication techniques based on text and colors are proposed. These techniques generate session passwords and are resistant to dictionary attack, guessing, shoulder-surfing attack and social engineering attacks. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration during login time based on the grid displayed a session password is generated. ColorLogin is a graphical passwords method to develop more effective, user friendly and secure.. In doing so it aims to motivate the user with a fun, friendly interface designed to improve user experience and provide acceptable login time. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

REFERENCES

[1] Haichang Gao, Sidong Wang, Xiyang Liu, Hongang Liu, and Ruyi Dai. Design and Analysis of a Graphical Password Scheme.2009 Fourth International Conference on Innovative Computing, Information and Control.
[2] Haichang Gao, Xiyang Liu, Ruyi Dai, Sidon Wang and Xiuling Chang. Analysis and Evaluation of the ColorLogin Graphical Password Scheme. 2009 Fifth International Conference on Graphics and Image.
[3] M Shreelatha, M Shashi, M Anirudh, MD Sultan Ahmer and V Manoj Kumar. Authentication Schemes for Session Passwords using Color and Images. International Journal of Network Security & its Applications. (IJNSA), Vol 3, No.3, May 2011
[4] Ashish Joshi Sonu Kumar and R H Goudor. A more Multi-factor Secure Authentication Scheme based on graphical authentication.2012 International conference on Advances in Computing and Communications.
[5] Phen - Lan Lin, Li-Tung Weng and Po-Whei Huang. Graphical Passwords Using Images with Random Tracks of Geometric Shapes.2008 Congress on Image and Signal Processing.

