Usage of Colors and Images for Authentication to avoid Shoulder Surfing

Dr. K N Narasimha Murthy , Apoorva C, Trupti
Dept. of ISE, City Engineering College, Bangalore
murthy_knn@Yahoo.co.in, apoorva2092@yahoo.co.in, trupthi.amarnath@gmail.com

Abstract

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 alternative techniques 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. 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.

Keywords: *Authentication, Session Passwords, Shoulder Surfing*

1. 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. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices**.** In this paper, two new authentication schemes are proposed for PDAs. 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. This paper is organized as follows: in section 2 related works is discussed; in section 3 the new authentication schemes are introduced; security analysis is done in section 4; conclusion is proposed in section 5.

2. Related Work

Dhamija and Perrig[1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in figure 1.

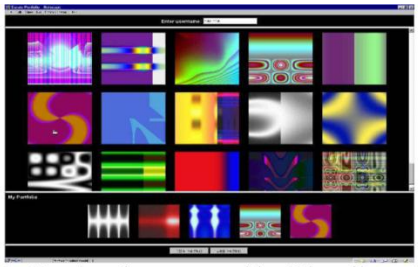

Figure 1: Random images used by Dhamija and Perrig

This system is vulnerable to shoulder-surfing. Pass face [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.

Figure 2: Example of Passfaces

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. Jermyn, et al. [3] proposed a new technique called "Draw- a-Secret" (DAS) as shown in figure 3 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.

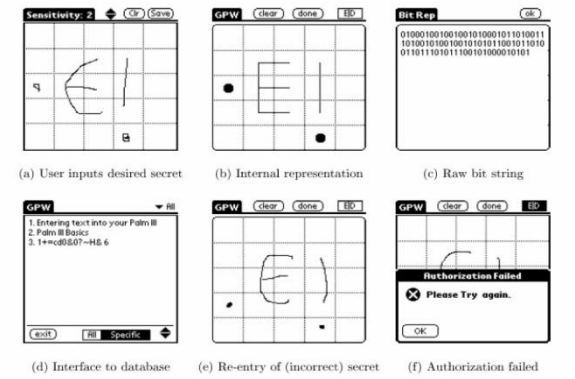

Figure 3: DAS technique by Jermyn

Syukri [4] developed a technique where authentication is done by drawing user signature using a mouse as shown in figure 4. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. The disadvantage of this technique is the forgery of signatures. Drawing with mouse is not familiar to many people; it is difficult to draw the signature in the same perimeters at the time of registration.

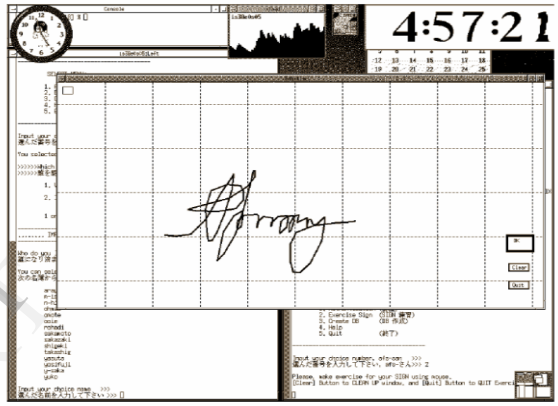

Figure 4: Signature technique by Syukri

Blonder [5] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Passlogix [6] extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity.

Haichang et al [7] proposed a new shoulder-surfing resistant scheme as shown in figure 5 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.

Figure 5: Haichang's shoulder-surfing technique

Figure 5: Haichang's shoulder-surfing technique

Wiedenback et al [8] describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks as shown in figure 6. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large.

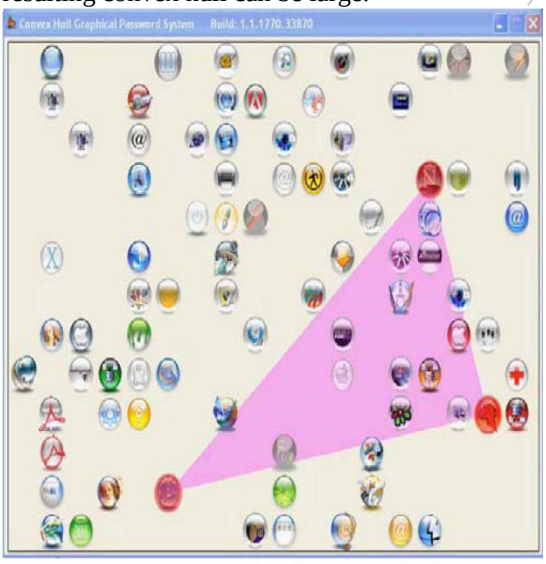

Figure 6: Example of a convex hull

Figure 6: Example of a convex hull

Jansen [9, 10] proposed a graphical password scheme for mobile devices. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the no. of images is limited to 30, the password space of this scheme is not large. Weinshall and Kirkpatrick [11] 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 [12] designed a technique known as "pass doodle". This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen. To overcome the shoulder-surfing problem, many techniques are proposed.

Zhao and Li [13] proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al [14] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the pass objects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants. More graphical password schemes have been summarized in a recent survey paper [15]. Zheng et al [16] designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.

3. New Authentication Schemes

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.

3.1 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.

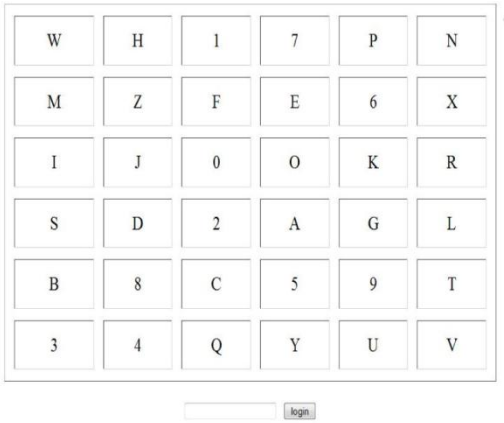

Figure 7: Login interface

Figure 7 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.

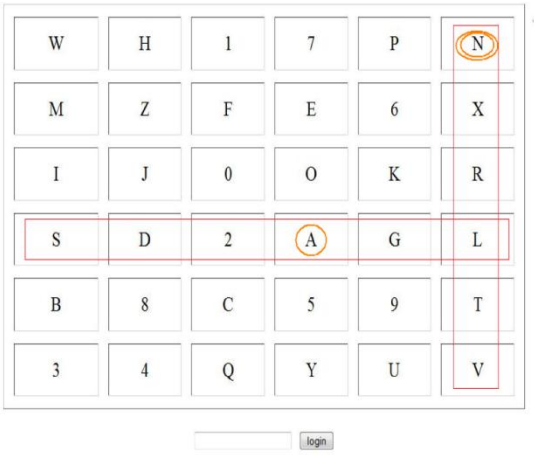

Figure 8: Intersection letter for the pair AN

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 8 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.

3.2 Hybrid Textual Authentication Scheme

During registration, user should rate colors as shown in figure 9. 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.

Figure 10 shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid.

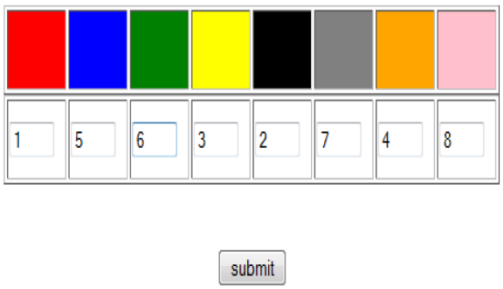

Figure 9 : Rating of colors by the user

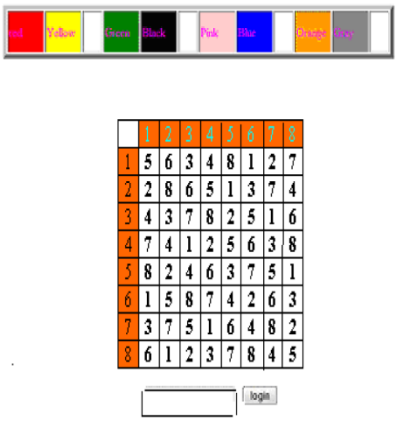

Figure 10: Login interface

The number in the intersection of the row and column of the grid is part of the session password. Consider the figure 9 ratings and figure 10 login interfaces for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e. **3**. The same method is followed for other pairs of colors. For figure 10 the password is "3573**"**. Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

4. Security Analysis

As the interface changes every time, the session password changes. This technique is resistant to Shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

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 fail towards our authentication systems because session passwords are used for every login.

Shoulder Surfing: These techniques are Shoulder Surfing Resistant. 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. 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 8^4.So these are resistant to shoulder surfing.

Guessing: Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 36^4. 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.

Brute force attack: These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

Complexity: The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 368. In the case of the Hybrid Textual Authentication Scheme the complexity depends on colors and ratings. The complexity is 8! If ratings are unique, otherwise it is 8^8.

5. Experimental Study

We conducted the user study of the proposed techniques with 10 participants for each technique. As the techniques are new, first the participants were briefed about the techniques. They were given demonstrations for better understanding purpose. Then each user was requested to login. After that, the usability study was conducted with the students in two sessions.

The sessions were conducted in time frame of one week. Table 1 shows the registration time for each technique. Table 2 shows the log-in time for each technique for the first session of user study. Table 3 shows the log-in time for the second session which was taken after one week of first session.

Table 1
Registration time for passwords

Technique	Avg	Min	Max
Hybrid Textual Authentication	58	48.8	78.4
For pair-based authentication, registration is similar to existing authentication			

Table 2

Login time for correct passwords at session1

Technique	Avg	Min	Max
Pair based authentication	29.95	24.6	43.26
Hybrid Textual Authentication	47.2	28.5	72

Table 3
Login time for correct passwords at session 2

Technique	Avg	Min	Max
Pair based authentication	26.25	18	40.4
Hybrid Textual Authentication	39.16	26.4	63.5

It is observed that, as the user gets practiced over, he is able to login without any problem. If the user is able to remember the password or ratings of colors, the schemes are resistant to shoulder surfing. The easiest way to remember ratings for colors is to use some concept or story and this leads to successful login in the Hybrid Textual Authentication.

6. Conclusion

In this paper, two authentication techniques based on text and colors are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. 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. 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] R. Dhamija and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
[2] Real User Corporation: Pass faces. www.passfaces.com
[3] Jermyn, I., Mayer A., Morose, F., Reiter, M., and Rubin. "The design and analysis of graphical Passwords" in Proceedings of USENIX Security Symposium, August 1999.
[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written With Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[5] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.
[6] Passlogix, site http://www.passlogix.com.
[7] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing
[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodsky, N. Memon, "Design and longitudinal evaluation Of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.
[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.
[10] W. Jansen, "Authenticating Users on Handheld Devices "in *Proceedings of Canadian Information Technology Security Symposium*, 2003.
[11] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.
[12] J. Goldberg, J. Hangman, V. Sazawal, "Doodling Our Way to Better Authentication", CHI '02 Extended abstracts on Human Factors in Computer Systems, 2002.
[13] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.
[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.
[15] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.
[16] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and Text" Journal of Computers, vol.5, no.5 May 2010.