Authentication Schemes for Session Passwords using Colors

Nita Dorage, Bhakti Sawant
Department of Information Technology, Terna Engineering College, University of Mumbai, Mumbai, Maharashtra, India

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.

Manuscript received April 5, 2016
Manuscript revised April 20, 2016

In this paper, new authentication scheme is 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 work 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. Literature Survey

We studied the working behavior of already existing authentication systems. Each of these applications offers different features and limitations. 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 he user has to identify the pre selected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing.

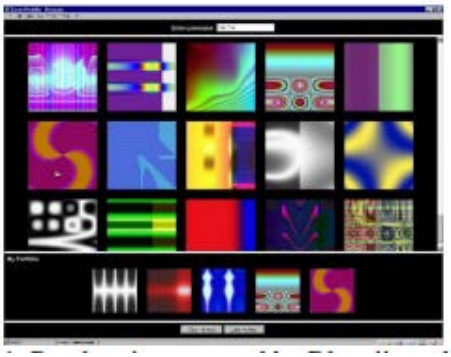


Figure 1: Random images used by Dhamija and Perrig

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.

Figure 2: Example of Passfaces

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.

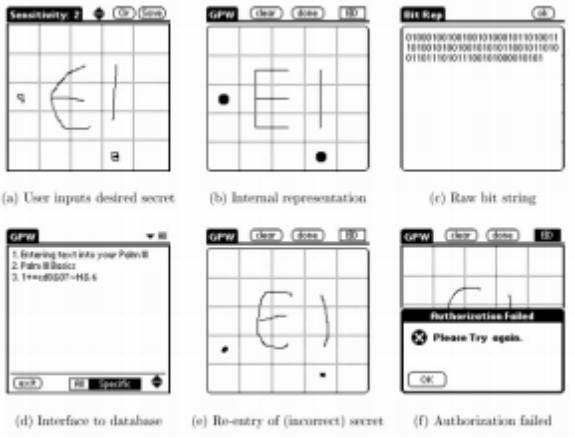


Figure 3: DAStechnique by Jermyn

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 stagethe 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

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

Wiedenback et al [8] describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks as shown in figure6. 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.

Figure6: Example of a convex hull

3. Proposed System

Hybrid Textual Authentication Scheme:
This scheme can be used where security is of main concern, for example ATM, Banking, mail etc.

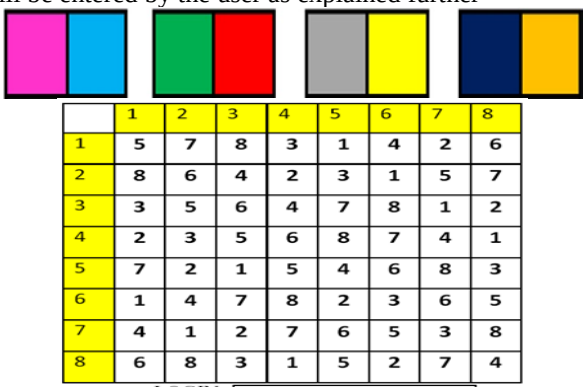
- The proposed Authentication technique is consisting of following 3 phases:
  1. Registration phase
  2. Login phase
  3. Verification phase

During registration, user will fill the registration form and with that an interface of 8 colors will be displayed. User should rate colors as shown in figure 7. The User is required to rate colors from 1 to 8 sequentially or randomly. Same rating can be given to different colors.
User can rate colors according to his interest (sequential as shown in figure 7(a) or random as shown in figure 7(b)). This rating will be sent to users email, in case if user forgets it.

figure 7(a) : sequential rating of colors by the user

figure 7(b): random rating of colors by the user

During login phase, when the user enters his username and passwoed, system will verify from database whether that user is exising or not, if it is exising user then an interface is displayed based on the colors selected by the user at registration time. This interface is generated containing 4 pairs of colors as shown in figure 8. Each pair of color represents the row and the column of the grid. The pairs are randomly generated for each session. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. based on this pairs and 8x8 grid, seperate password is generated for each session, i.e. a new session password for every new session, giving a secure authentication system. Password will be entered by the user as explained further



	1	2	3	4	5	6	7	8
1	5	7	8	3	1	4	2	6
2	8	6	4	2	3	1	5	7
3	3	5	6	4	7	8	1	2
4	2	3	5	6	8	7	4	1
5	7	2	1	5	4	6	8	3
6	1	4	7	8	2	3	6	5
7	4	1	2	7	6	5	3	8
8	6	8	3	1	5	2	7	4

Figure 8 : login interface generated having color pairs and 8x8 grid

Let say user has rated pink as 8, blue as 4, green as 3, red as 2 and so on as shown in figure 7(a). then in the pair first color represents row, and second column. User need to find intersection point as shown in the figure and enter as shown in the figure. The password for each session is different as per random pairing of colors. This provides a more secure system.

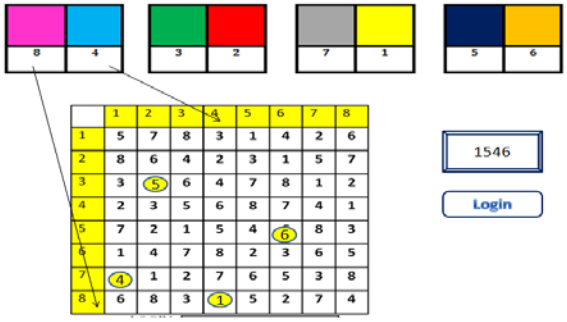


Figure 9: example showing password for paring for figure 7(a)

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

Shoulder Surfing: These techniques are Shoulder Surfing Resistant. 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 .

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.

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. 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 88.

5. Conclusion

In this paper, authentication technique based on text and colors is proposed. These technique generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing.. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated.

Acknowledgment

It gives the authors great pleasure in expressing our gratitude to all those people who have supported us and had their contributions in making this dissertation possible. First and foremost, we express our profound sense of reverence to our guide Prof.Smita Deshmukh, for his constant guidance, support, motivation and untiring help. We are also thankful to Head of the Information Technology Department and Principal of Terna Engineering College for their support and valuable suggestions. We are also thankful to all staff members of Information Technology Department, without whom the completion of this report would have been impossible.

References

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th

[2] Real User Corporation: Passfaces. www.passfaces.com..

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999 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

[4] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[5] Passlogix, site http://www.passlogix.com.

[6] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing

[7] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy,N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127

[8] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.

[9] W. Jansen, "Authenticating Users on Handheld Devices"in Proceedings of Canadian Information Technology Security Symposium, 2003.