ISSN:0975-9646

Suwarna Jungari et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3355-3358

Authentication Session Password Scheme Using Texts And Color

Suwarna Jungari, Vrushali Bhujbal, Shital Sonawane, Supriya Bhujbal, Prof. Shital Salve

Department of Computer Engineering ICOER College of Engineering, Pune Maharashtra.

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 consider this problem, text can be combined with colors to generate session passwords for security purpose. 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 protect data from dictionary attack, shouldering etc. These methods are suitable for Personal Digital Assistants.**

Index Terms: **Authentication, session passwords, pair-based authentication scheme; hybrid textual authentication scheme**

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 we cannot remmember. Studies have shown that users tend to pick short passwords that are easy to remember. Unfortunately, these passwords can be guessed easily. [1]The another approache 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. [2]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. [3]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 techniques are proposed for PDAs. [4]These techniques authenticate the user by session passwords. Session passwords are passwords that are used only one time. Once the session is terminated, the session password is no longer useful. That means next time this password cannot waok.For every login process, user's input different passwords. [1]The session passwords provide better security against dictionary and brute force attacks. The proposed authentication schemes use text and colors for generating session passwords.

2.RELATED WORK

[2]Dhamija and Perrig proposed a graphical authentication scheme where the user has to identify the predefined images to prove user's authenticity. In this system, the user selects the number of images for purpose of selecting password. In the login phase the user has to identify the preselected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing.

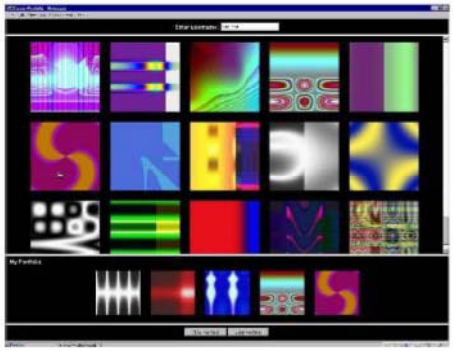
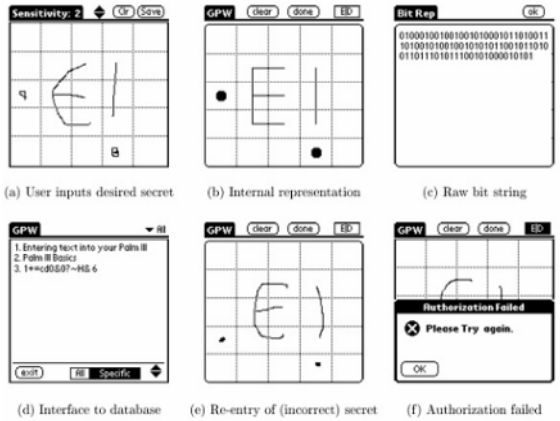


Figure 1: Random images used by Dhamija and Perrig

Pass face 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 Pass faces

Proposed a new technique called “Draw- a-Secret” (DAS) as shown in figure3 where the user is required to redraw 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.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Figure 3: DAS technique by Jermyn

[3]Syukri 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 designed a graphical password scheme where the user must click on the approximate areas.

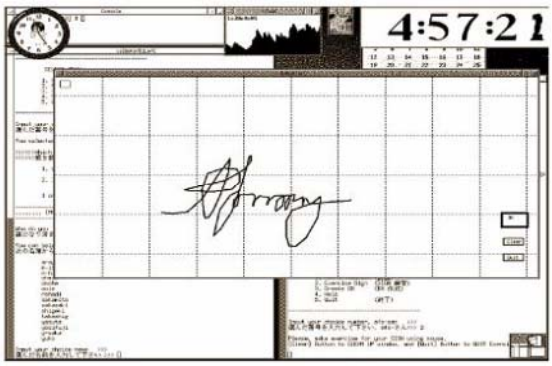


Figure 4: Signature technique by Syukri

[4]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. [3]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

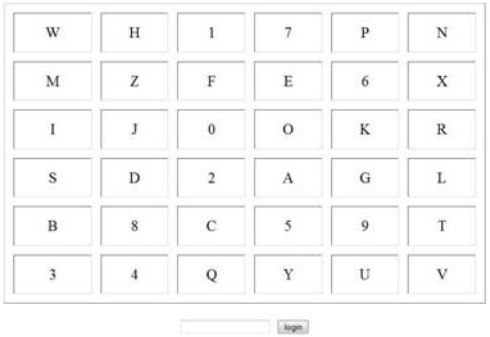
[1]Wiedenbacketal describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks as shown in figure 6. [1]A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number 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.

3. New Authentication Schemes

Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his/her 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 grid 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. [1]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 also special symbols. These are randomly placed on the grid and the interface changes every time but new session must be generates.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Figure 6: Login interface

Figure 6 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, digits and special symbols.

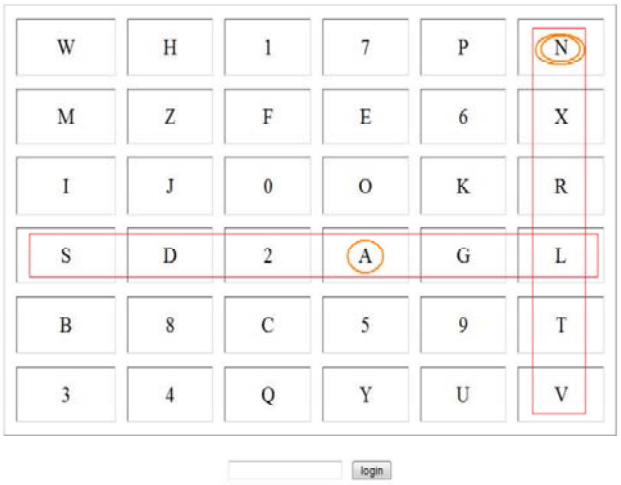


Figure 7: Intersection letter for the pair AN

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 7 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

[1]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. [3]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 8

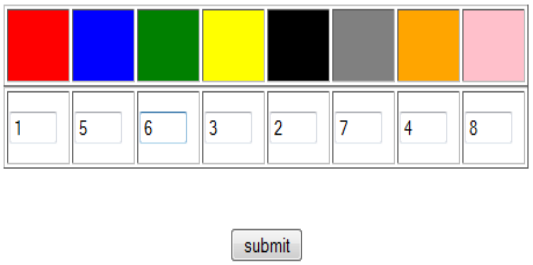


Figure 8 : Rating of colors by the user

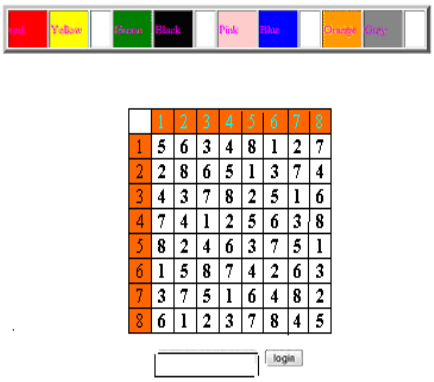


Figure 9: Login interface

[3] Figure 9 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. The number in the intersection of the row and column of the grid is part of the session password. Consider the figure 8 ratings and figure 9 login interface 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 9 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.

Safe Mode

The Safe mode comprises of the Pair based Authentication scheme and the One-Time- Password technique. [4]The user can login either through the Normal mode or the Safe mode as per his requirement.

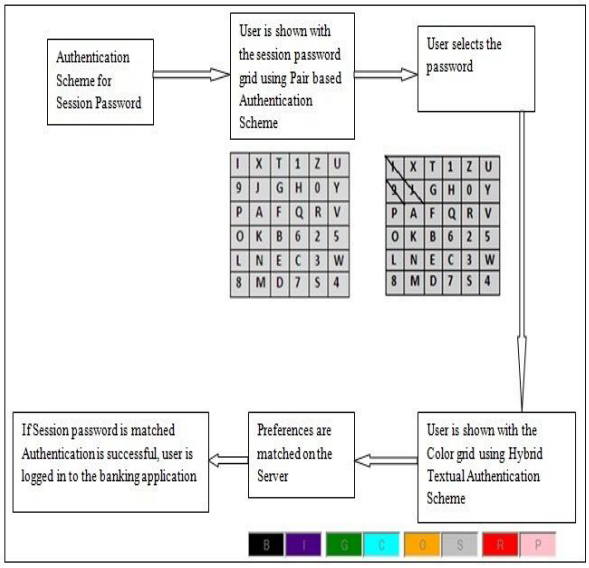


Fig. 10: Architecture of the proposed system

4. SECURITY ANALYSIS

As the interface changes every time, the session password changes. [2]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 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. 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 88.

5. 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 and password easy to remmember.

REFERENCES

[1] VAISHNAVI PANCHAL, CHANDAN P. PATIL a user study using "*Authentication schemes for session password*" March 2013.

[2] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini "authentication technique for engg session passwords with colors" 2012.

[3] M SREELATHA , M SHASHI , M ANIRUDH "Authentication Schemes for Session Passwords using Color and Images" May 2011.

[4] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

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

[6] 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.

[7] 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.

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

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

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