K.Nivetha, M. Muthumeena, R. Srinivasan / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.1611-1615

Authentication Mechanisim For Session Passwords By Imposing Color With Text

K.Nivetha[1], M. Muthumeena[2], R. Srinivasan[3]
[1,2]PG Scholar, Dept of CSE, Vel Tech DR.RR & DR.SR Technical University, Avadi, Chennai-62.
[3]Assistant Professor, Dept of CSE, Vel Tech DR.RR & DR.SR Technical University, Avadi, Chennai-62.

ABSTRACT

The most common method used for authentication is Textual passwords. But textual passwords are in risk 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 helpless 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.

Key words: Authentication, session passwords, shoulders surfing, Eves dropping.

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. Arbitrary 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 broken. 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. Personal Digital Assistants (PDs) 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.

2. RELATED WORKS

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. 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. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

Akula and Devisetty's algorithm is similar to the technique proposed by Dhamija and Perrig. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's.

Figure 1.Random images used by Dhamija and Perrig.

"Pass face" is a technique developed by Real User Corporation the user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces (Figure 2). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

Figure 2. An example of Pass faces.

Davis, et al. Studied the graphical passwords created using the Pass face technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Pass face password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password.

Jermyn, et al. proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password (figure 4). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.

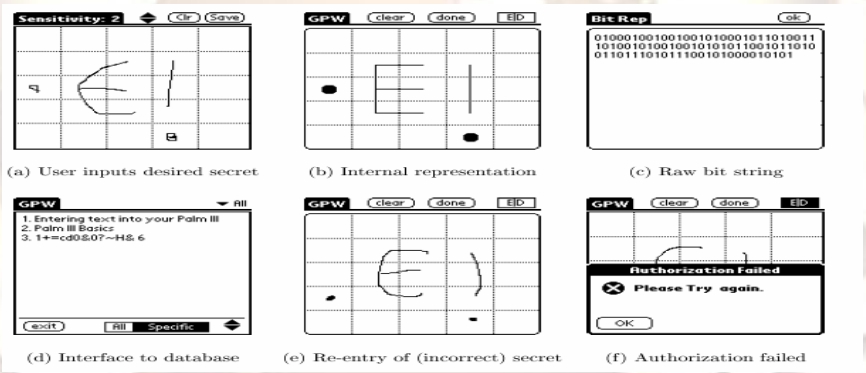

Figure 4. (DAS) technique proposed by Jermyn.

To overcome shoulder-surfing challenge, many methods have been proposed. One of such technique is designed by Man, et al[10].In this system, the user selects many portraits as the pass objects. Each pass object is allotted an inimitable code. During the verification process, the user has to input those unique codes of the pass objects in the login interfaces presented by the System. Though the scheme resists the hidden camera, the user has to memorize all pass object codes. In this way, many other graphical authentication schemes and their drawbacks are presented in a latest survey paper

3. NEWEST METHODS FOR AUTHENTICATION

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 METHOD

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.

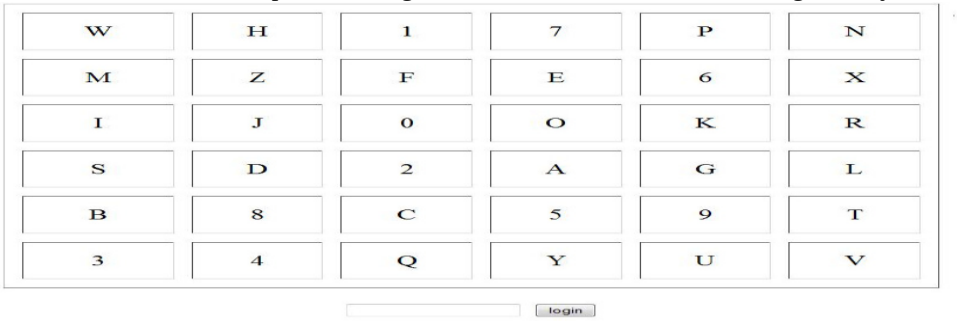

Figure 5: Login interface.

Figure 5 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.

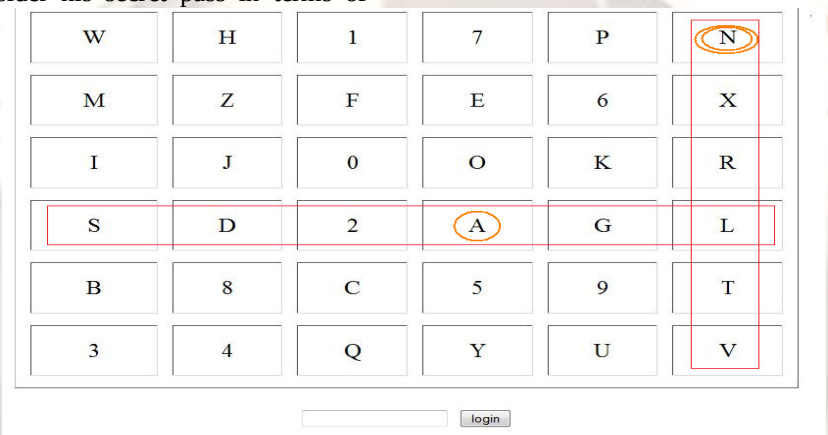

Figure: 6 Intersection letter for the pair AN

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. Figure 6 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 7. The User should choose the colors from 1 to 8 and they 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 18. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

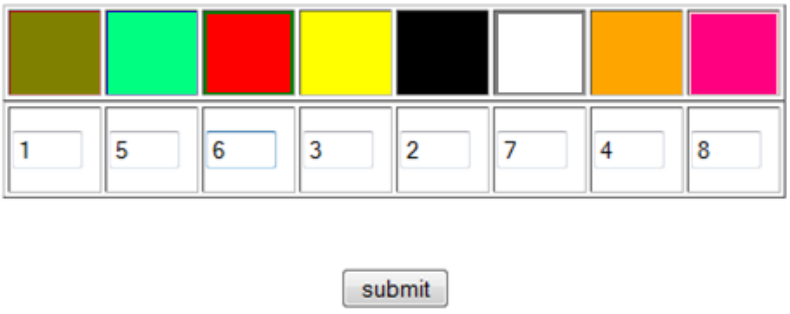

Figure 7: Choosing the colors by the user

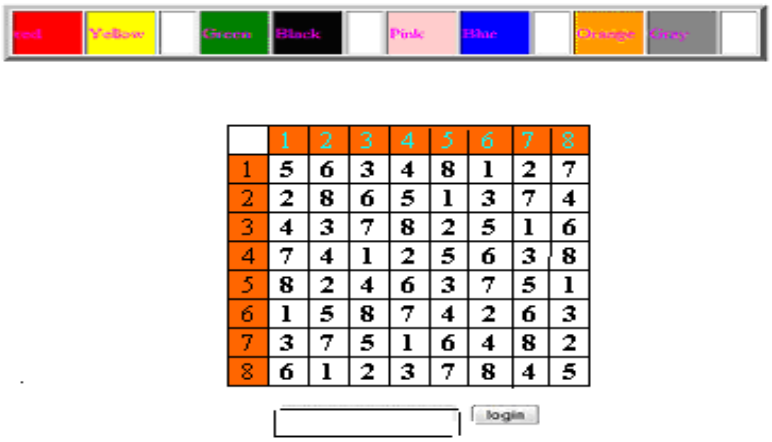

Figure 10: Login interface

Figure 8 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 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 8 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. ANALYSIS FOR SECURITY

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 Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains.

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.

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: 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.

[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. Brodskiy, 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. Hagman, 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.

[17] M. Sreelatha, M. Shashi , M. Anirudh ,MD Sultan Ahamer 1, Network Security & Its Applications Vol.3, No.3, May 2011.