IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. II (Jan. 2014), PP 36-42
www.iosrjournals.org

Authentication Scheme for Session Password using matrix Colour and Text

Mr. Sagar A. Dhanake, Mr. Umesh M. Korade, Mr.Chetan P. Shitole,
Mr. Sagar B. Kedar, Prof. V. M. Lomte
Under Guided
(Comp Dept., PVPIT, Pune, India)
(Comp Dept., PVPIT, Pune, India)

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.*
Keywords: *Authentication; dictionary attack; shoulder surfing; session passwords; pair-based authentication scheme; hybrid textual authentication scheme; draw-a- secret.*

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. 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(PDAs) 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.

II. Related Works

Word-based passwords introduced in the early years are subjected to various attacks as mentioned in the former section. Besides this, many graphical authentication schemes have been evolved based on the requirements and the pitfalls associated with the prior existing authentication methods. Let us have a brief description of the various prevailing and proposed graphical authentication methods. Blonder [5] proposed a graphical password technique, in which the password is generated by allowing the user to click on different positions on an image. During authentication, the user has to click on the estimated areas of those locations. Later, this idea was prolonged by 'pass-point system'where the predefined boundaries are excluded and arbitrary images are supported. Consequently, for constructing password, the user can click over any region on the image. A tolerance around each chosen pixel is evaluated. To be authenticated, the user has to click within the tolerance level of the pixels chosen.

Syukri [6] designed a scheme in which authentication is carried out by sketching out the user signature with mouse. This scheme involves two levels, registration and verification. While registering, the user draws his signature using mouse, the system then extracts the signature area. During the verification level, it acquires the

user signature as input, performs normalization and finally extracts the parameters of the signature. But this scheme is associated with several disadvantages such as forgery of signatures, inconvenience while drawing with mouse, difficulty in sketching the signature in the same perimeters at the time of registration. Besides this, a new graphical authentication method has been designed by Dhamija and Perrig[1]. This method, while creating the password allows the user to select certain number of pictures from a set of random images. Then, during login, the user has to recognize the preselected portraits from the set of images. But this method is liable to shoulder-surfing.

Passface[7] is an approach proposed by the Real User Corporation in which the user is allowed to choose four images of human faces from the face database as their password. During the verification phase, the user is provided with a grid of nine faces, one already chosen during the registration and eight decoy faces. The user identifies the selected face and clicks anywhere over it. This course of action is repeated for four times, and the user is ascertained as genuine if he recognizes all faces accurately.

A new innovative authentication scheme is proposed by Jansen [8, 9] for mobile devices. While creating the password, the user chooses a theme of snapshots in thumbnail size and the sequence of those snapshots is fixed as password. As each thumbnail is associated with numerical value, the sequence of images form numerical password. The only drawback with this method is that the password space is not large, as no of images is limited to 30.

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 [11].

III. PROJECT WORK

The project illustrated in this paper is entirely based on the idea of session passwords. Here, the main objective of this project is to provide security to the confidential files, folders in computing devices through session passwords. It includes 3 phases: registration, primary level authentication, secondary level authentication (draw-a-secret). The process of figuring out the validate person is accomplished in the following manner:

3.1 REGISTRATION

When we run the application, a login form turn up, allowing the user to enter the username. The form appeared consists of three buttons-register, login, close.

Figure1: Login Screen

Figure 2: Form for entering password directed to mobile

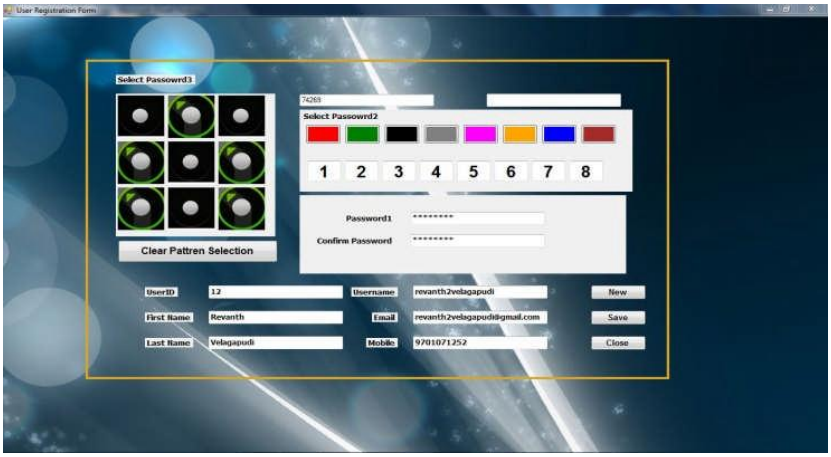

Figure3: Registration Form

If the user is already a registered one, then clicking on the "login"button would advance him to the second phase of the application. If the user is not a registered member, then on doing the above action would generate a message box conveying "username doesn't exist". Thus, in order to make use of the application, the person must get registered by the admin.

Consequently, on clicking the "register" button on the login form would display a window allowing the user to enter his mobile number. On submitting the mobile number, a password is directed to his mobile by the admin.

Then, the user has to write down the password in the interface shown subsequently, and has to click on the "register" button below that interface. On doing so, registration form appears.

Thereafter, the user enters textual password whose minimum length is 8 and it contains even number of characters. If the user violates this protocol, then a message box expressing the fault with the textual password is displayed. This password is to be remembered as pair-based password, also known as secret pass. Besides this, the user has to rank the colors portrayed as color grid of 8 colors in the registration form. The rank (from 1 to 8) associated with each color has to be remembered as the hybrid textual password. Along with these, graphical password (draw-a-secret) using the 3X3 grid is sketched. Moreover, basic details like first name, last name, mobile number and email-id are submitted by the user.

Clicking the "new" button in the registration form would automatically generate the user-id based on the existing users. On ticking the "save" button, all the information inserted by the user is stored on to the database. Thereby, again the login form is displayed, where the user now clicks on "login" button advancing him to the second phase of the application.

3.2 Primary Level Authentication

The users who are allowed to proceed to the primary level authentication are generally of two types: admin and users registered by the admin. Both are permitted to follow the same approach for the primary level authentication. Ticking the "login button", a window is displayed presenting the two modes namely, pair-based authentication scheme and hybrid textual authentication scheme for validating the primary level.

Figure 4:Login Selection Window

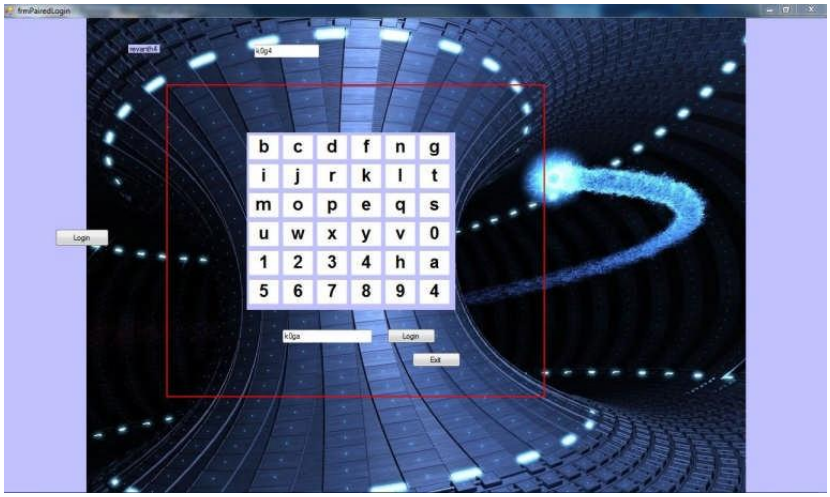

Figure 5: Pair-based Login Screen

The user can then select any one of the methods that is convenient for him in order to clear the primary level authentication. There is "return to login" button which on clicking would move back to the login screen. The "close application" on the top right corner is used for closing the application.

3.3 Pair-based Authentication Scheme

In the course of registration, the user submits the secret pass. The minimum length of the secret pass is 8 and it should contain even number of characters. During the primary level authentication, when the user chooses the pair-based authentication scheme, an interface consisting of 6X6 grid is displayed. The grid contains both alphabets and numbers which are placed at random and the interface changes every time. The mechanism involved in the pair-based authentication scheme is as follows: Firstly, the user has to consider the secret pass in terms of pairs. The first letter in the pair is used to select the row and the second letter is used to select the column in the 6X6 grid. The intersection letter of the selected row and column generates the character which is a part of the session password. In this way, the logic is reiterated for all other pairs in the secret pass [4]. Thereafter, the password inputted by the user i.e. the session password is now verified by the server to authenticate the user.

3.4 Hybrid Textual Authentication Scheme

During registration, the user gives rankings (1to8) to colors in the color grid which is considered as the hybrid textual password. In primary level authentication, when the user selects the hybrid textual authentication scheme, an interface is displayed. The interface consists of 8X8 number grid in which numbers from 1 to 8 are placed haphazardly. In addition to this, a color grid is also displayed containing 4 pairs of colors. Both these grids changes for every session. The logic involved in this scheme is that the rating given to the first color of every pair represents a row and the rating given the second color in that pair represents a column of the 8X8 number grid. The number in the intersection of the row and column of the grid is the part of session password. This procedure is repeated for the remaining color pairs in the color grid [4].

In both the cases, if the session password entered by the user is correct, then he is permitted to face the secondary level authentication. Otherwise, the user is prompted to re-enter the session password according to the secret pass and hybrid textual password.

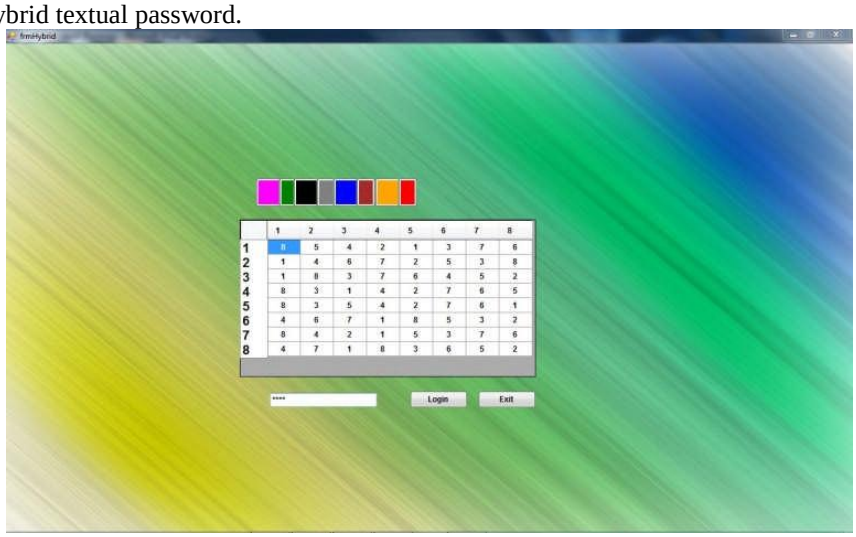

Figure 6: Hybrid Textual Login Screen

3.5 Secondary Level Authentication (Draw-a-secret)

In this phase, the process of authentication is different for admin and the registered users. Initially, for both the types of users, a 3X3 grid consisting of dots is shown.

The user has to draw a sequence, known as draw-a-secret joining the dots [12]. In case of a normal registered user, if the sequence drawn during authentication matches with the sequence drawn during the registration phase, then the user is given the permission to access the confidential files. He can even change the passwords if he wants to do so.

Whereas in case of the admin, once the sequence matches, then a message is shown requesting to insert the pen drive to the system.

Figure 8: User Privileges to Confidential Files

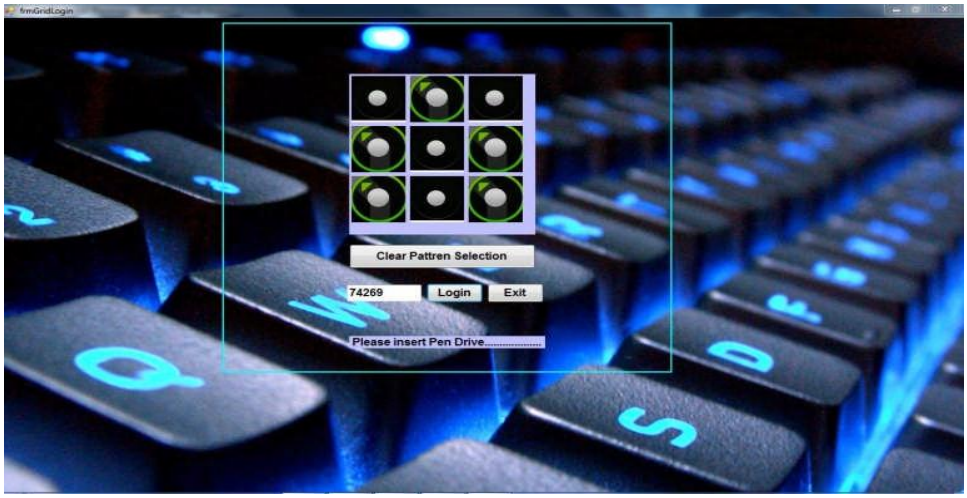

Figure9: Message showing admin to insert Pen Drive

Figure10: Admin Privileges for Accessing Files

A file containing the password is made hidden in that drive. If that password is identical to that written in the back-end instructions, the admin is given the privilege to view, update and perform various operations on the files as shown in the above figure. In case, if the pen drive is lost, then clicking on the "lost drive" button, the password is sent to the admin mobile phone. Now the admin can use a new pen drive having the file with the password sent to mobile, again in hidden mode.

For both the types of users, if the draw-a-secret is wrong, then a message "sequence doesn't match" is indicated to the user. Thereby, the user would click on "clear the selection" button and would make another try.

In this way, security is given to confidential data in an organization, thereby giving the access rights only to the certain set of employees in it.

IV. CONCLUSION

Generally, there are many drawbacks associated with the textual passwords such as brute-force and dictionary attacks. Similar is the case with the graphical passwords which includes shoulder-surfing and are very expensive to implement. As such, we have proposed the idea of utilizing session passwords for authentication. For this purpose, we had made use of both the textual and graphical password techniques. In this paper, we have implemented two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords. Associated with these techniques is the draw-a-secret graphical method employed for security issues.

Acknowledgements

The authors would like to thank project guide Prof. V.M. Lomate and H.O.D. Prof Y.B. Gurav PVPIT, Pune (India).for their guidelines and involving in research.

References

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

[2] 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.

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

[4] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer,V Manoj Kumar "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA),Vol.3, No.3,May2011.

[5] G. E. Blonder. Graphical passwords. *United States Patent 5559961*, 1996.

[6] 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.

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

[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.

[10] 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.

[11] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.

[12] 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.

[13] Y. Zhang, L. Wu, Rigid Image Registration by PSOSQP Algorithm, Advances in Digital Multimedia, vol.1, no.1, pp.4-8, 2012.

[14] Tejaswi Lalitha Surepeddi, K. Gowtham, A. Ramakrishna, D. Aruna Kumari, Design, Implementation of Network Based Authentication Mechanisms, Advances in Information Technology and Management, vol.1, no.2, pp.44-48, 2012.

[15] P. Vikram Varma, Siva Pillalamarri Prasad, R. Leela Kumari Virtual laboratory through internet, Advances in Information Technology and Management, vol.1, no.2, pp.60-65, 2012.