An Overview: Passwords using Text, Color and Images Techniques Discussion, Implementation and Comparison

Pardeshi Sachin N.
Asst. Professor, Dept. of Computer Engineering
R.C. Patel Institute of Technology, Shirpur

Vipul D. Panjabi
Asst. Professor, Dept. of Computer Engineering
R.C. Patel Institute of Technology, Shirpur

ABSTRACT
Textual passwords are the widespread method used for confirmation. But textual passwords are defenseless to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as substitute techniques to textual passwords. Most of the graphical schemes are susceptible to shoulder surfing. To tackle this problem, text can be combined with images or colors to create passwords for authentication. In this paper, we discussed technique to generate passwords using text, colors and images which are opposing 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 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[17,18].

International Journal of Network Security & Its Applications (IJNSA), this paper, two new authentication schemes are proposed for PDAs.[18] 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[17,18]. The authentication schemes use text images and colors for generating passwords new way. This paper is organized as follows: in section 2 related work is discussed; in section 3 related project work done; in section 4 the new authentication schemes are introduced; security analysis is done in section 5; in section 6 conclude the paper.

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 ascertain 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. This system is vulnerable to shoulder-surfing.

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

Syukri [4] developed a technique where authentication is done by drawing user signature using a mouse. 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.

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 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.

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

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 "passdoodle". 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. 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.

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.

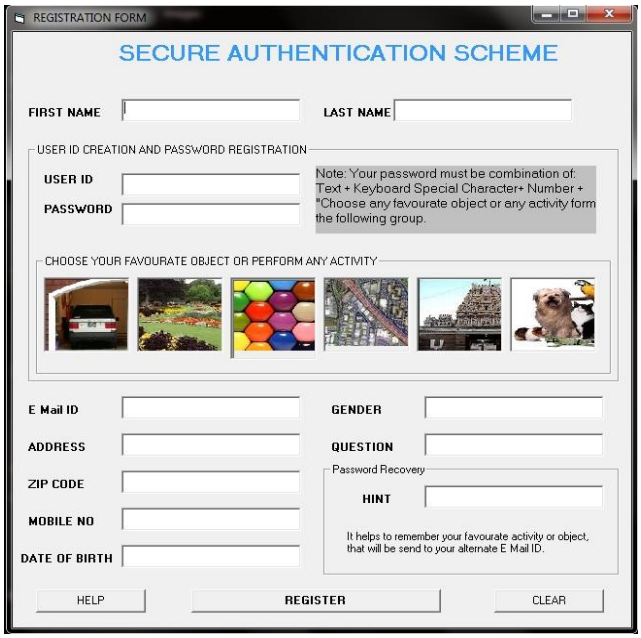

Fig 1: Registration Form

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.

Again he has to go any group shown in Fig 1, the first image is for garage if user enters in the garage he could use different tools and he has to remember only which tool he has used in this way password added in the password field. We have created different category to choose flowers from the garden, favourate color, location, favourate holy places and favourate pets. After clicking on this images a special character is added in the password field that can be create your password more complex. Special character as shown in figure 2.

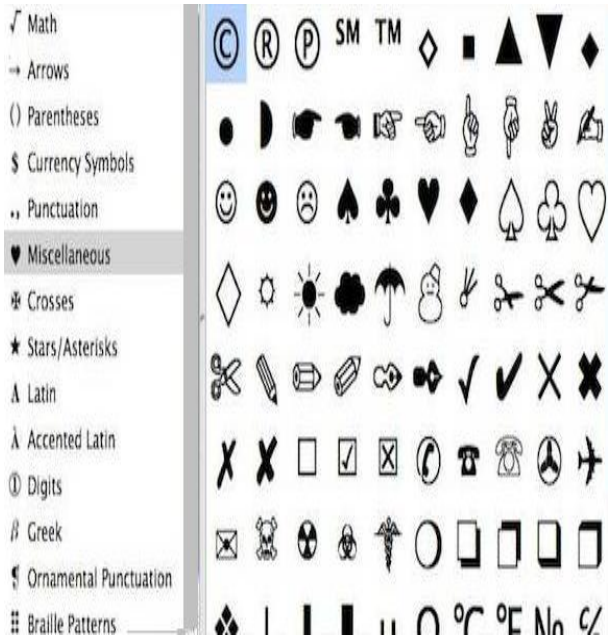

Fig. 2 Special Characters

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 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.

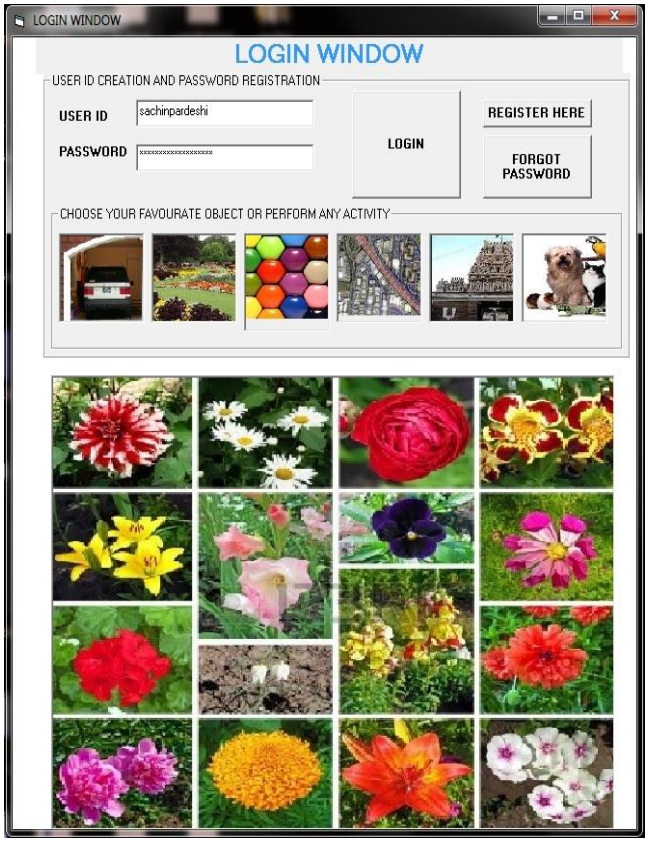

Fig 3: Login Form

4. 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.

4.1 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. Passwords Hits are generated based on this secret pass. During the login phase, when the user forgot his password the textual selection can generate a password and can send hint answer to the alternate email id.

User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs.

4.2 Hybrid Textual Authentication Scheme

During registration, user should choose any object from different group. The User should choose the colors, flower, temple, pets etc. and he can remember it as because he chooses according to his interest. Same rating can be given to different colors. During the login phase, when the user enters his username and insert a password which is combination of images, color, location or specific activity if all are right in password window allowed to go for login.

5. 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 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 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. 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.

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.

7. 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-

[5] Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

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

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

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

[9] 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.

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

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

[12] 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.

[13] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[14] 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.

[15] 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.

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

[17] 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.

[18] Suwarna Jungari, Vrushali Bhujbal, Shital Sonawane, Supriya Bhujbal, Prof. Shital Salve,"Authentication Session Password Scheme Using Texts And Color" International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, pp. 3355-3358.