A BETTER SCHEME FOR AUTHENTICATION USING SESSION-PASSWORDS

[1]Priyada.P[2], Smitha.J C
[1]PG Student, Dept. of Computer Science and Engineering,
Lourdes Matha College of Science and Technology, Thiruvananthapuram
[2]Assistant Professor,
Dept. of Computer Science and Engineering,
Lourdes Matha College of Science and Technology, Thiruvananthapuram

ABSTRACT
The most common method used for authentication is Textual passwords. But textual passwords are vulnerable to dictionary attacks, eves dropping, social engineering and shoulder surfing. An alternative technique to textual passwords is Graphical passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, authentication using session passwords are introduced, where text can be combined with images or colors to generate session passwords for authentication. Session passwords are one time passwords which means they can be used only once and every time a new password is generated. In this paper, three techniques are proposed to generate session passwords using text, colors and pictures (images) which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

KEYWORDS—*Authentication, session passwords, shoulder surfing*

1. INTRODUCTION

Authentication establishes our identity so that we can obtain the set of rights. The mechanism identifying an individual, based on a username and password is known as authentication. Textual or Alphanumeric passwords are the most common method used for authentication. The vulnerabilities of this method are eves dropping, dictionary attack, social engineering and shoulder surfing. Random and lengthy passwords can make the system more secure. But the problem is the difficulty of remembering those lengthy passwords. Commonly users tend to use short passwords. Even though these passwords are easy to remember, but can be easily guessed or cracked.

Graphical passwords and biometrics are alternative techniques to textual passwords. But these two techniques have their own disadvantages. Biometrics authentication schemes which includes finger prints, iris scan or facial recognition. These techniques are also not yet widely adopted since such systems can be expensive and the identification process can be slow. Also graphical schemes are vulnerable to shoulder surfing. To address this problem, authentication scheme based on session passwords is introduced where text can be combined with images or colors to generate session passwords. Session passwords are dynamic and onetime passwords since it can be used only once and every time a new password is generated. In this paper, three techniques are proposed to generate session passwords using text, colors and pictures which are resistant to shoulder surfing. These schemes are suitable for Personal Digital Assistants.

2. CURRENT APPROCHES FOR AUTHENTICATION

Dhamija and Perrig [1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove the authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, the user has to identify the pre selected images for authentication from a set of images during login. This system is vulnerable to shoulder-surfing.

Passface [2] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other images. Since there are four user selected images it is done for four times.

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. the user is authenticated only when the drawing touches the same grids in the same sequence. The vulnerability to this authentication scheme is shoulder surfing.

Syukri[4] developed a technique where the authentication is done by drawing user signature by using a mouse. This technique includes two stages such as registration and verification respectively. At the time of registration, the user draws his signature using a mouse, after that the system extracts the signature region. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. The drawback of this technique is the forgery of signatures. Most of the people are not familiar in drawing with mouse ; at the time of registration, it is difficult to draw the signature in the same perimeters.

To overcome the shoulder-surfing problem, many techniques are proposed. Zhao and Li [5] proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is that, in the login stage, user must find his original text passwords in the login image and click inside the invisible triangle region. The system has high level security which integrates both graphical and textual password scheme.

Man, et al [6] proposed another technique which is shoulder-surfing resistant. Here a user chooses many images

as pass-objects. The pass-objects have variants and a unique code is assigned to each of them. In the authentication stage, the user must type the unique codes of the pass-objects variants in the scenes provided by the system. Even though the scheme shows perfect results in resisting hidden camera, the user has to remember code with the pass-object variants.

3. NEW PROPOSED AUTHENTICATION SCHEMES

Generally, Authentication technique involves of 3 phases:1.registration phase, 2.login phase and 3.verification phase. During registration, user enters the username and password in the first method and rates the colors in the second method. Then the user has to enter the password during login phase, which is based on the interface displayed on the screen. The system verifies the password which is entered by the user during login by comparing with content of the password generated during registration.

A. Text Pair Based Authentication Scheme

During registration user submits his password. This password is called as secret pass or pass key. The pass key 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. This grid is called magic matrix. The matrix is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid. The interface changes every time.

The user has to consider the secret pass which is given during registration phase 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. The intersection letter of the row and column is part of the session password. This is repeated for all pairs of the pass key. If the password is correct, the user is allowed to enter in to the system.

B. Hybrid Textual (Color-based) Authentication Scheme

During registration, user should rate colors shown in the color panel. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". The user can give same ratings to different colors. During the time of login, when the user enters his username, an interface is displayed in the login screen which is based on the colors selected by the user. This interface consists of grid of size 8×8. This grid contains digits 1-8,alphabets from 'a' to 'z' and special symbols which are placed randomly in grid cells. There is also a strips of colors will be displayed in the login screen as shown

in figure 4. This color grid consists of 4 pairs of colors. Each pair of color indicates the row and the column of the grid.

The login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8,alphabets from 'a' to 'z' and special symbols are 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 interface grid. The number in the intersection of the row and column of the grid is part of the session password. We can include both albhabets and special symbols in the interface grid. For every login, both the interface grid and the color grid get randomizes so the session password changes for every session.

C. Picture Based Authentication

During registration, user has to create a picture profile. The user should select 2 pictures according to his/her choice from the picture box, which contain total 9 (3x3 matrix) pictures. From the selected pair of pictures, there will be total 4 different variations of these 2 pictures (total 8 images) will be shown in the right side window. Here the user have to name each images accordingly and should have to remember for further login process. After successfully creating the picture profile, during the login process, the user should enter his/her username, along with this; there will be a 4x4 matrix containing 16 images will be displayed. from this picture matrix, user have to select the 2 appropriate pictures that he was selected and named during picture profile creation and name it as he named during profile creation. If the image names are valid, then the user is valid and he can successfully login.

4. SECURITY ANALYSIS

As the interface changes every time, the session password also changes. This technique is resistant to shoulder surfing.Dictionary attack is not possible and it is not applicable for dynamic passwords,. Hidden camera attacks are not applicable to PDAs because it is difficult to capture the interface in the PDAs.

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

B. 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.

C. Guessing

Guessing can't be a threat to the pair based because it is hard to guess secret pass. 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.

D. Brute force attack

These schemes are particularly resistant to brute force attack due to use of the dynamic session passwords. The use of these will take out the traditional brute force attack out of the possibility.

5. RESULTS AND DISCUSSION

Fist of all ,the user has to create his/her profile for text pair based authentication and color based authentication respectively. For picture based authentication, the user has to create a picture profile during registration. The pass key should be of even number of characters. He should have to remember this pass key for further login.

For Color based authentication, during profile creation ,the user has to rate the colors shown in the grid and this color rate should also to me remembered by the user. Here the user submits the pass key as "mn62".She has rated the colors as shown in fig1.

In Text pair based authentication, when the user who has created his profile submits his username and then a matrix or grid of size 6x6 will be displayed.Here the user have to consider her passkey which is 'mn62',in this pass key,cosider 'mn' as one pair and '62' as another one pair.Then find out the intersection points of these 2 pairs form this grid and this intersection points will be the session password.Here "B" is the intersection point of the pair 'mn' and "U" for the pair '62'.

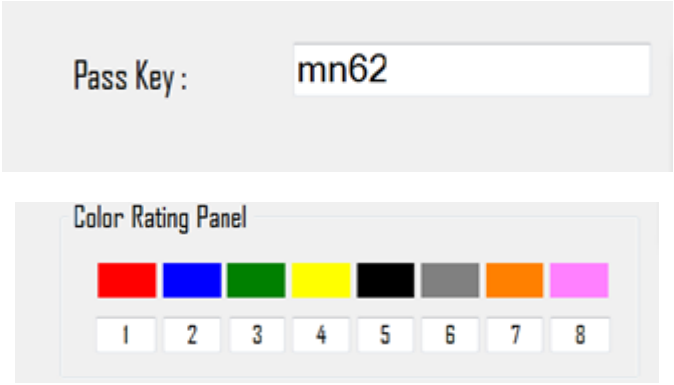

Fig 1 Profile Creation

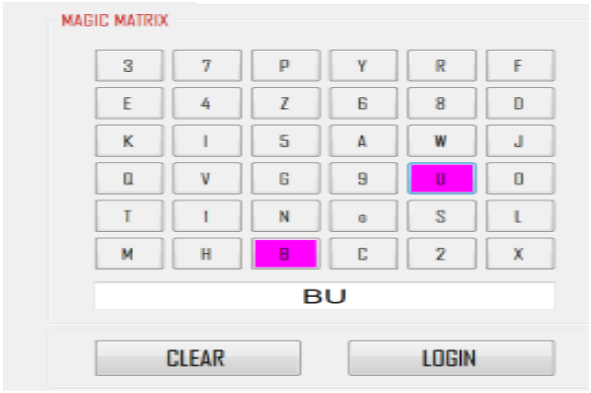

Fig 2 Text Pair Based Authentication

Fig 3 Color Based Authentication

For Color based authentication,when the user enters his username then two interfaces will be displayed on the login screen.One is the color grid for 8 colors which are in the form of 4 pairs and another one grid is of size 64 which consists of numbers,characters and special symbols as shown in Fig 3.

The user has to consider the color ratings which she has done during profile creation and using the color grid panel she has to enter the password in this login form.The user has to first consider the color panel.Lets take the first pair which is pink and black.She has rated 6 for "pink" and 7 for "Black".so she has to consider the 7th entry in the 6th row .Here the entry is "L" .So the first character in the session password will be "L".This is repeated for all 4 pairs of colors.

For Picture Based authentication, first step is picture profile creation.This is done during Registration phase.The user who has created the picture profile only can login using picture based authentication scheme. The user should select 2 pictures according to his/her choice from the picture box, which contain total 9(3x3matrix) pictures as shown in Fig 4. From the selected pair of pictures, there will be total 4 different variations of these 2 pictures (total 8 images) will be shown in the right side window. Here the user have to name each images accordingly and should have to remember for further login process.

During the login process, the user should enter his/her username, along with this; there will be a 4x4 matrix containing 16 images will be displayed as shown in Fig 5. from this picture matrix, user have to select the 2 appropriate pictures that he was selected and named during picture profile creation and name it as he named during profile creation. If the image names are valid, then the user is valid and he can successfully login.

Fig 4 Picture Profile Creation

Fig 5 Picture Based Authentication

6. CONCLUSION

In this paper, 3 authentication techniques based on text and colors and pictures are proposed mainly for PDAs. These techniques generate session passwords and which are resistant to dictionary attack, brute force attack and shoulder-surfing. 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. For picture based scheme, the user should select and name the images shown in the grid during the login phase. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness. These techniques can also be developed as windows application such as a folder locker. These schemes will be best suitable for all the situations where security of data is more important than access/login time.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication", 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] 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.
[5] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme,", *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.
[6] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey", Proc. ACSAC'05.