International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Secure Authentication for Password Selection against Key and Mouse Tracker

Miss Shubhangi P. Joge[1], Miss Deepali M. Khatwar[2]

Dept. of computer science and Engineering[1,2], Agnihotri college of Engineering, Nagthana road, Wardha(MH)[1,2]

Shubha.joge@gmail.com[1], deepalikhatwar@gmail.com[2]

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 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, three techniques are proposed to generate session passwords using text, grids and colors which are resistant to shoulder surfing, key and mouse tracker. These methods are suitable for Personal Digital Assistants.

Index Terms: Authentication, session passwords, shoulder surfing, keyboard tracker, mouse tracker.

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 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 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. LITERATURE REVIEW

Three Level Authentication Scheme by Kunal Mulwani,, Saurabh Naik [5]. Textual passwords exist since 1960. From then, they have been a common mechanism to authenticate users. Applications that we use in our day to day life use textual passwords to authenticate users. The main motivation behind the graphical password is the fact that human can easily remember graphical password as compared to textual. Graphical passwords tend to be more secure as compared to textual passwords.

A New Graphical Password Scheme Resistant to Shoulder-Surfing by Haichang Gao [4]. The proposed shoulder-surfing resistant scheme can be considered as an improvement of Story, as it keeps most of the advantage of Story and achieves stronger security. Like Story, our scheme is based on recognition, an easier memory task than recall, and suggests users to create a story for sequence retrieval. Instead of direct input, it depends on users drawing a curve across their password images (passimages) in order. The curve containing both pass-images and decoys guards against shoulder-surfing attacks by human observation. Using a drawing input method, our scheme is designed to empower users to log in their mobile devices quickly. The user can remember the connection between the pass-images by mentally constructing a story.

Figure 1 shows a prototype of our scheme, which uses a template of 24 identically sized images, grouped into a 4× 6 matrix. In Figure 3, the pass-

images labeled by blue rectangles are in identical order with that in original image.

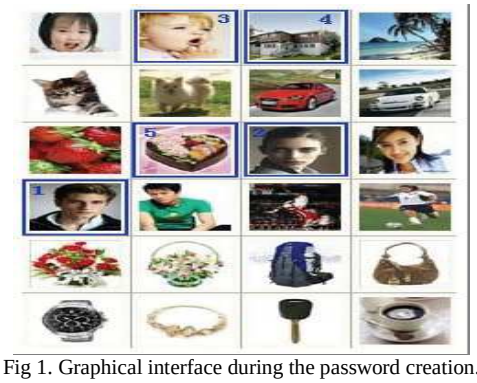

Fig 1. Graphical interface during the password creation.

A hidden story may be “a couple and the son want to share a cake at their house”. To log in, a user should draw a curve to orderly cross the pass-images from the given head image to the tail image.

The new shape based textual authentication scheme consists of three steps:

- password creation
- password entry
- password verification

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 Identification System Using Signature Written with Mouse by Syukri [8] developed a technique where authentication is done by drawing user signature using a mouse as shown in figure 3. 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

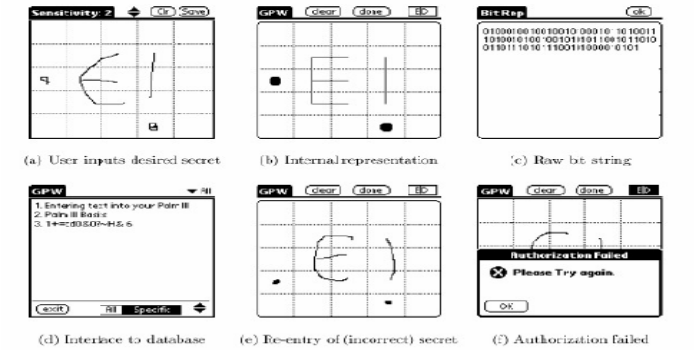

Fig 2. DAS technique by Jermyn

The design and analysis of graphical passwords by Jermyn, et al. [7] proposed a new technique called “Draw- a-Secret” (DAS) as shown in figure 2 where the user is required to re-draw the pre-defined picture 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.

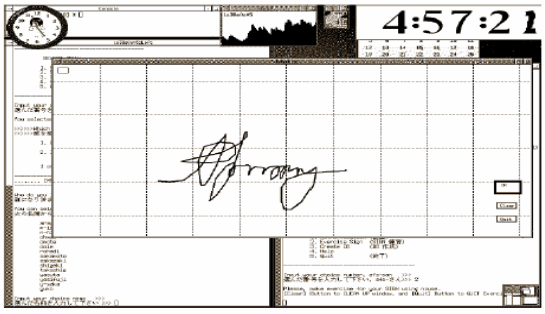

Fig 3: Signature technique by Syukri

3. SYSTEM ARCHITECTURE

Authentication technique consists of 3 phases:
(1) Registration phase
(2) Login phase
(3) 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 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. 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 4(a) 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.

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 4(b) 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.

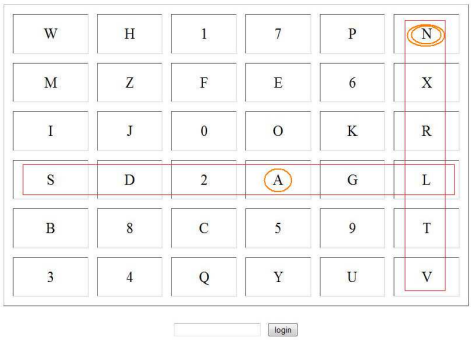

Fig 4(a). Login interface

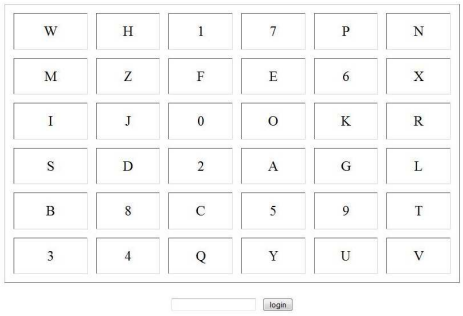

Fig 4 (b). Intersection letter for the pair AN

3.2 Gridding based Authentication Scheme

At the time of registration the user enter the image. Then select grid value and apply on the image. The image is now converted into gridding format having 3 x 3 grids. Means 9 grid images are get from original image as shown in figure 5(a) and 5(b).

Fig 5(a). Original image

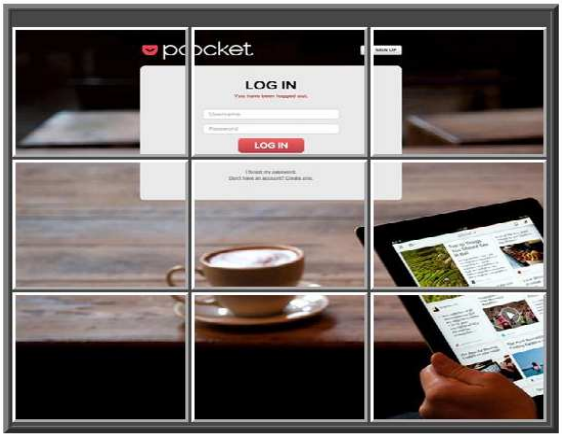

Fig 5(b). Grid image

The user select grid patterns as per their views. When enter in login phase then the original grid image is now converted into 5 X 5 grids. Means total 25 grid images are formed. Then user select appropriate grid block of image as shown in figure 6, as he enter in registration phase. Also maintain the sequence of grids.

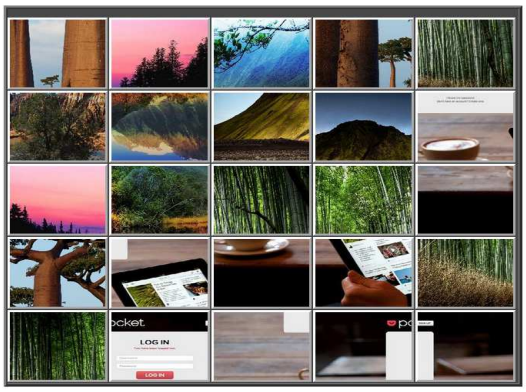

Fig 6. 16 extra grids added to the original grid image and make 5 X 5 grids

3.3 Hybrid Textual Authentication Scheme

During registration, user should rate colors as shown in figure 7. 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. The interface also contains strips of colors as shown in figure 8. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

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 8 ratings and figure 8 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 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.

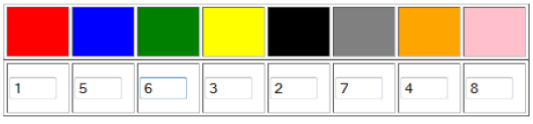

Fig 7. Rating of colors by the user

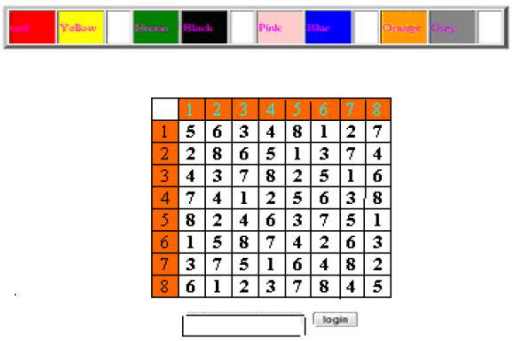

Fig 8. Login interface

4. SECURITY ANALYSIS

As the interface changes every time, then session password also changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable.

4.1 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.

4.2 Shoulder Surfing

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. So these are resistant to shoulder surfing.

4.3 Guessing

Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 36. 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.

4.4 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.

4.5 Key tracker

One of the tricks spyware uses to spy on you once it's on your system is to intercept keystrokes to find out what you're doing and maybe capture user names and passwords. The first thing you need to know is that every keyboard logger uses a feature that is built into Windows called a "keyboard hook." So this technique prevent from this keyboard tracker.

4.6 Mouse tracker

The second level of authentication prevent from mouse tracking. Mouse tracking (also known as cursor tracking) is the use of software to collect users' mouse cursor positions on the computer. This goal is to automatically gather richer information about what people are doing, typically to improve the design of an interface. Often this is done on the Web and can supplement eye tracking in some situations.

5. CONCLUSION

In this paper, three authentication techniques based on text, grids and colors are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack, keyboard tracker, and mouse tracker 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] M sreelatha , m shashi , m anirudh ,md sultan ahamer, v manoj kumar Authentication Schemes for Session Passwords using Color and Images.

[3] Sreelatha Malempati, Shashi Mogalla USER AUTHENTICATION USING NATIVE LANGUAGE PASSWORDS

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

[5] Kunal Mulwani1, Saurabh Naik2, Navinkumar Gurnani3, Dr. Nupur Giri4, Prof. Sharmila Sengupta 3LAS (Three Level Authentication Scheme)

[6] Priyanka Kedar, Vrunda Bhusari Pair & Hybrid Based Authentication Technique using PBKDF2

[7] 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.

[8] 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.