© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Survey of Various Password Authentication Schemes

Shritika Waykar[1], Tejaswini Barhate[2], Nidhi Iche[3]
[1]Department of Computer Engineering, DYPCOE, Pune, Maharashtra, India
[2]Department of Computer Engineering, DYPCOE, Pune, Maharashtra, India
[3]Department of Computer Engineering, DYPCOE, Pune, Maharashtra, India

ABSTRACT

Textual passwords generally are used for authentication. Graphical password is introduced opposite method to textual passwords. Most users are aware with textual password than pure graphical password. Shoulder-surfing is a known hazard where an attacker can seizure a password by direct show or by listening the verification session. Text can be combined with alphabet, digit, images or colors to generate session passwords for authentication. In early days Textual passwords are used for security of session but these passwords are vulnerable to the various attacks like Dictionary attack, Shoulder surfing, eves dropping, etc. Further graphical passwords and bio-metric password methods are created for authentication. These two methods are good to carry out but they have their own disadvantages. Such as it requires additional period for login and more expensive respectively. Session password strategy in which the passwords are used only once for each and when session is terminated the password is no longer in use. The session password scheme uses Pair Based Authentication scheme for generating session password. The paper discusses various approaches of passwords authentication schemes.
Keywords: Pair based scheme, Session Passwords, Shoulder Surfing, Dynamic Grid.

I. INTRODUCTION

Social networking has become an important factor in our life, which allows us to connect with the families and friends. Nowadays mobile are showing an vital role in day by day life. They have come up with the tag linear anywhere; anytime that has given hike to the term Mobile Social Network. Social networking has become an important factor in our life, which allows us to connect with the families and friends. Nowadays mobile are showing an vital role in day by day life. . They have crop up with the identification line anywhere; anytime that has given hike to the term Mobile Social Network. Authentication is the main step to access any social website, where user have to put username and password i.e. some credential to the system so that the they will understand genuine user is accessing the website. Many schemes and techniques are available to provide the authentication. Authentication process divided into Token based authentication, Biometric based authentication and Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical passwords[9]. There are graphical password schemes that have been proposed which are support to shoulder surfing but have their own drawbacks is taking more time for user to login or usability issues. The user is authenticated using session password. Session passwords are the password that is provided to authenticate the user for a session. Session passwords are used only once. Every time the users enter a session he has to input different password. Once the session is over that password becomes is of no use for next session and the current session gets terminated. Session password provide more security as every time the session start a new password is created and they are not prone to dictionary attacks ,brute force attacks and shoulder surfing attacks. In Authentication, the user has to submit correct credentials which are already stored in the system.

II. Authentication Techniques

In Authentication, the user has to submit correct credentials which are already stored in the system. Then user will access the system. There are various ways of authentication techniques i.e. textual passwords, Graphical passwords and Biometrics.

- **Textual Password:**

Among the various authentication techniques textual password is popular. It consists of the string of alphabets and special characters. Generally the users have tendency to choose simple passwords i.e. Spouse's name, maiden name, building name etc. User can choose any arbitrary or lengthy password to avoid such attacks. But studies have found that they are not easy to remember. There are various attacks possible on the textual passwords like Brute Force attack, Eavesdropping, Dictionary attack, Social Engineering, Key Logging and Shoulder Surfing etc[6].

- **Graphical Password:**

Graphical passwords were introduced to overcome the attacks faced by textual passwords mostly shoulder surfing, key logging etc. Various graphical password schemes were introduced by many authors.[9] In such a scheme the user have to enter the username. After that the graphical objects will be displayed on the screen. Depending on the scheme either user have to place images from random to correct order which were preselected by user while registration. Using mouse, touch pad, touch screen user has to select the objects. Also signatures can be used for authentication. But even if the slight change is found the authentication is stopped. Though the system is secured compare to the textual passwords it has lots of disadvantages. User verifies or authenticate only when proper sketch is drawn. Extra sensitive key pads are required for such scheme. Also the time required in authentication process is longer. Graphical password authentication techniques are as follows:

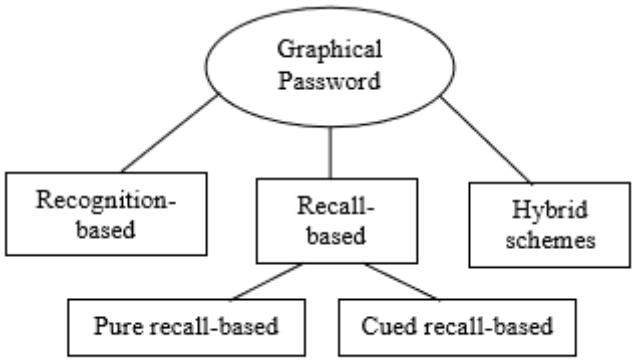

Figure 1: Graphical Password Authentication Techniques

A. Recognition-Based Technique:

In this category, users will select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images. Researches were done to find the memo ability of these passwords and it shows that the users can remember their passwords even after 45 days.

B. Pure Recall-Based Technique:

In this category, users have to reproduce their pay role without being given any type of hints or reminder. Although this category is very easy and convenient, but it seems that users can hardly remember their pay role. Still it is more secure than the recognition based technique.

C. Cued Recall-Based Technique:

In this category, users are provided with the reminders or hints. Reminders help the users to reproduce their pay role or help users to reproduce the pay role more accurately. This is similar to the recall based schemes but it is recall with cueing.

D. Hybrid Schemes:

In this category, the verification will be typically the combination of two or more schemes. These methods are used to overcome the disadvantages of a single scheme, such as spyware, shoulder sieving and so on.[10]

- **Biometrics Scheme**

The biometric scheme is used for authentication which is based on the image recognition process. In this scheme first the image is pre-processed and then matched with the database. Iris recognition, face recognition, thumbs recognition are the various types of biometrics. It is one of the good authentication schemes as it's real and unique. Also it doesn't have the fear to be stolen. But this scheme is expensive also the process is time consuming.

Biometric authentication systems are used in order to verify the claimed identity of a user based on his biometric characteristics. Although authentication information should be kept confidential, for biometrics this cannot be guaranteed since it is very easy to obtain biological information such as finger print, iris or face data through finger print marking or using a camcorder. In order to avoid the imitation attacks, biometric measurements should be performed in controlled environments, for instance under the supervision of an operator[4],[5].

III. METHODS AND MATERIAL

2.1 Dhamija and Perrig

Dhamija and Perrig 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 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 2. This system is vulnerable to shoulder-surfing.

Figure 2 : Random Images Used By Dhamija and Perrig

2.2 Passface Technique

Passface is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in Figure 3. Here, the user chooses four images of human faces as their pay role and the users have to select their pass image from eight other decoy images[2].

Figure 3: Example of Pass faces

2.3 Draw- a-Secret

Proposed a new technique known as "Draw- a-Secret" (DAS) where the user is required to re-draw the pretend picture on a 2D grid. If the drawing touches the same grids in the same steps, then the user is verified. This verification scheme is accessible to shoulder sieving[3].

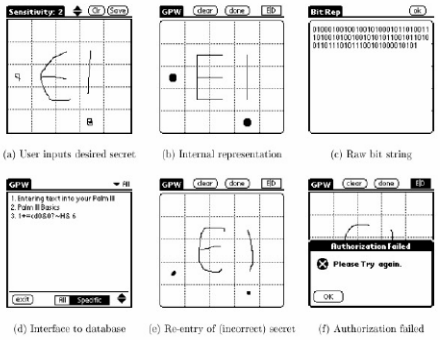

Figure 4: DAS technique by Jermyn

2.4 Hybrid Textual Authentication Scheme

During registration, user should amount colors as shown in figure 9. The User should amount 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 integrate is displayed based on the colors selected by the user. The login integrate consists of grid of size 8×8. This grid includes digits 1-8 placed about in grid cells. The integrate also contains strips of colors as shown in figure 10. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

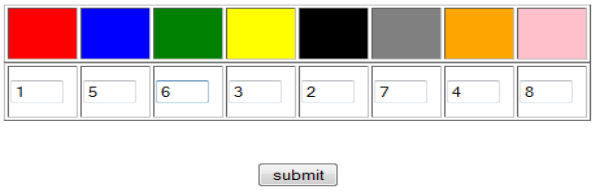

Figure 5: Rating of colors by the user

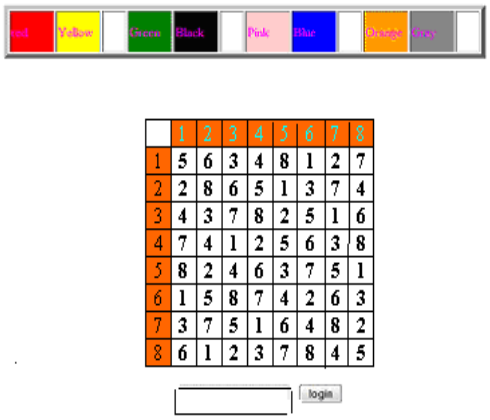

Figure 6: Login interface

2.5 Pair-based Authentication scheme

During registration user submits his payrole. Minimum length of the payrole is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session payrole are generated based on this secret pass. During the login phase, when the user enters his username an integrate 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 integrate changes every time.

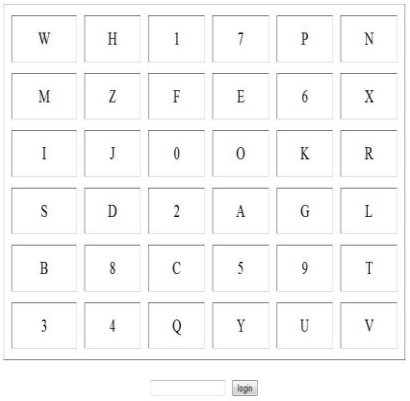

Figure 7 : Login interface

Figure 7 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.

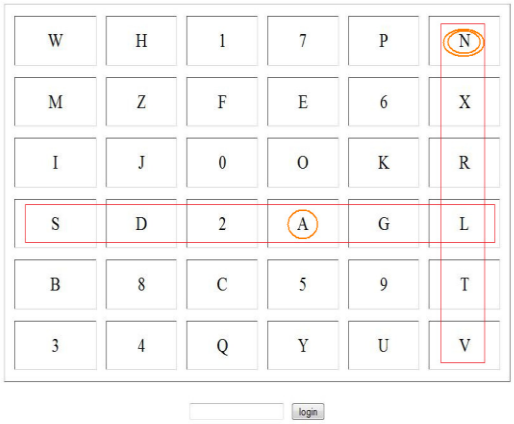

Figure 8 : Intersection letter for the pair AN

IV. RESULTS AND DISCUSSION

Table 1. shows textual passwords, graphical passwords, biometrics and Pair Based Dynamic Grid Authentication are compared in various parameters. From which it is clear that Pair Based Dynamic Grid Authentication requires low cost, it gives high protection level, processing time is also low and it doesn't require additional hardware. We can see that it is the best technique.

Table I. Comparison of Authentication technique

Authentication Schemes	Cost	Protect i-on Level	Processi ng Time	Additio n-al H/W Requir ed
1.Textual Password	Low	Mediu m	Low	No
2.Graphical Password	High	Mediu m	High	Yes
3.Biometric	High	High	High	Yes
4.Pair Based Dynamic Grid	Low	High	Low	No

Table II. Enlist the attacks possible on the above scheme. We can see from the table that except textual password all other schemes, too resist various attacks but their implementation cost is high. Again we can say that Pair Based Authentication using Dynamic grid is the best technique.

Table II. Attack on the Authentication technique

Authentication Scheme	Attacks	Resistant to Attacks	Cost
1.Textual Password	Eaves Dropping, Shoulder Surfing, Social Engineering, Key Logging, Guessing	-----	Low
2.Graphical Password	-----	Eaves Dropping, Shoulder Surfing, Social Engineering,	High
3.Biometric	-----	Eaves Dropping, Shoulder Surfing, Social Engineering, Key Logging	High
4.Pair Based Dynamic Grid	-----	Eaves Dropping, Shoulder Surfing, Social Engineering, Key Logging	Low

V. CONCLUSION

Thus textual passwords are the simplest way to handle the login process it is more prone to attacks. Other methods graphical password requires more processing time than the textual passwords hence lessen the performance. Also it provides medium security. Another traditional scheme, biometrics faces the challenge for maintaining the high precision equipments required for scanning iris, thumbprint, etc. Pair Based Dynamic Grid Authentication shows that it is efficient in reducing processing time by taking texts as the input. Also, shows the cost for designing the system is very less as no external hardware is required for the authentication process. It is resistant to many attacks and provides high protection level. The implemented authentication scheme is faster and more secured compared to the other methods in the market.

VI.REFERENCES

[1] Jay Patel, Prof. Ashil Patel, "A Research on Authentication Scheme for Session Password with colour Pairs and Grid compared with OTP," IJSRSET , Volume 2 , Issue 3 ISSN : 2395-1990

[2] Mr. Sagar A. Dhanake, "Authentication Scheme for Session Password using matrix Colour and Text", IOSR-JCE, Volume 16, Issue 1

[3] Reshma kadam, Swapnil kashit, "Authentication Scheme for Session password Using Hybrid and Paired Based Techniques", KJCOEMR, volume 1,issue 2,pp.175-182

[4] M.L. Gavrilova, "Biometric Based Authentication for Cyberworld Security", CDFAI, vol 2

[5] Vaclav Matyas and Zdenek Rıha, "Biometric Authentication Security and usability", NIST ,FIPS PUB 140-1/2

[6] Janhavi Thakur, Sheetal Rathi, " Pair Based Authentication using Dynamic Grid", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 ,Issue: 8 .

[7] S. Rajarajan, K. Maheswari, R. Hemapriya, S. Sriharilakshmi,"Shoulder Surfing Resistant Virtual Keyboard for Internet Banking", World Applied Sciences Journal 31 (7): 1297-1304, 2014 ISSN 1818-4952

[8] A. A. Doke, D. B. Wagh, S. H. Shaikh, Prof. S. S. Gawali, "Graphical and Pair Based Scheme for Authentication Using Session Password", International Journal of Advance Foundation And Research In Science & Engineering, Volume 1, March 2015.

[9] Priyanka S. Kedar, Vrunda Bhusari, "Using PBKDF2 Pair and Hybrid technique for Authentication", International Journal of Emgerging Research in Management and Technology ISSN:2278-9359(Volume-3,Issue-5).