ISSN:0975-9646

Shefali Amlani et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1420-1423

Session Authentication using Color Scheme

Shefali Amlani
Department Of IT
KJSCE, Vidyavihar (E)
Mumbai, India

Shweta Jaiswal
Department Of IT
KJSCE, Vidyavihar (E)
Mumbai, India

Suchitra Patil
Department Of IT
KJSCE, Vidyavihar (E)
Mumbai, India

***Abstract*- The most common method used for authentication is textual password, graphical passwords, biometrics etc. .The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. 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 as 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 but the drawback to this is most of them suffer from shoulder surfing and usability issues or taking more time for user to login or having tolerance. 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 device. In this Project, a new authentication scheme is 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.**

Keywords: Authentication, Security, Shoulder Surfing, Dictionary attacks.

I. INTRODUCTON

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 Project, a new authentication scheme is 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. LITERATURE SURVEY

Various comprehensive investigations on the existing authentication schemes have been accomplished. And it has been discerned that none of the recent authentication schemes can resist all sorts of attacks. With this outcome, this paper proposes an authentication schemes which overcomes all the existing authentication schemes. Literature review reveals all the studies that are done in past. Some of the authentication schemes are discussed as follows:

1. Dhamija and Perrig[1]

Proposed a graphical authentication scheme in which the user identifies the pre-defined images to prove the authentication of the user. In this scheme, during registration the user selects a set of images from a predefined set of images. Later on at the login time the user has to select the images that he had selected during the registration time to prove his authentication.
But this system is vulnerable to shoulder-surfing.

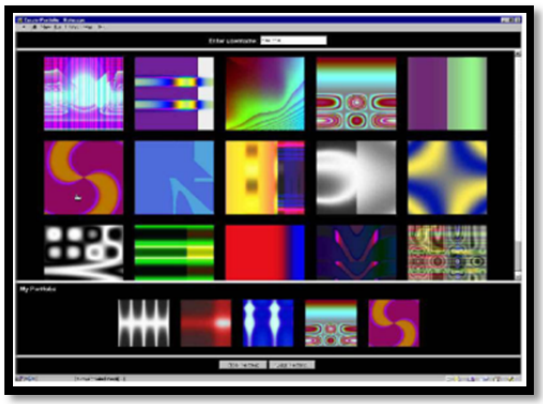

Fig. 1 Random images used by Dhamija and Perrig.

2. *Pass faces :*

Later on a new schemes was introduced known as Passfaces[2].In this scheme there is a grid of nine faces and the user to select on image from the grid.the user chooses four images of human as their password and have to select their pass image from the other eight images.since there are four user select images it is done four times.But this schemes was very easy to attacks by guessing or trying for number of time.

Fig. 2 Example of Passfaces

Futher studies were made on authentication schemes and a new scheme was proposed known as "Draw-a-Secret"(DAS) by Jermyn, et al. [3].The user has to draw a picture on the grid at the time of registration. The user has to draw the same picture on a 2D grid at the time of login. If the drawing of picture touches the same grid in same sequence .the users gets authenticated. But this scheme was prone to shoulder surfing attacks.

C. Draw –A-Secret

Similar to this a same scheme was introduced by Syukri [4].This authentication scheme was based on the principle that the user has to draw his signature by using mouse. This scheme had two stages of implementation viz.the registration phase and the verification phase. At the time of registration the user draws a signature that is extrated by the system.At the time of registration the signature is taken as an input and normalization is done and then the parameters are extracted and cheking is done and the user is authenticated if the parameters gets matched.But drawing with mouse is not so easy and acutals parameters cannot be matched with the signature that was drawn at the registration time.this schemes is prone to forgery of signature.

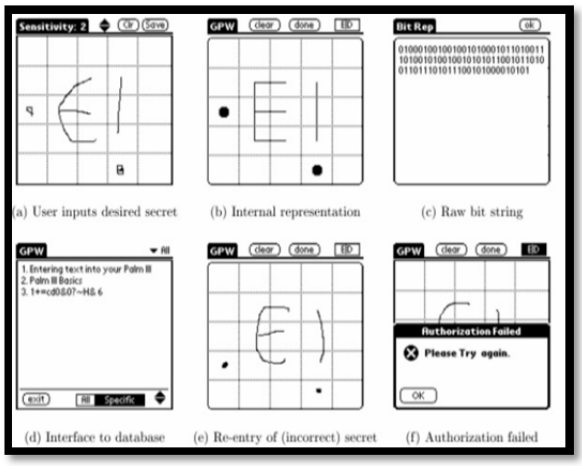

Fig. 4 DAS technique by Jermyn

1. Story-Scheme

To overcome this shoulder surfing attacks a scheme was proposed by Haichang et al [7].This schemes is the combination of DAS and Story schemes. The user has to draw a curve along the images to prove their authenticity.

Fig. 4 Haichang's shoulder-surfing technique

2. I) Graphical Passwords.

To overcome shoulder surfing attacks a new graphical password scheme was introduced by Wiedenback et al [8].the user has to recognise the pass objects and click in the convex hull formed of the pass objects. If the password had to be made large then it becomes crowded.

II) Graphical Passwords.

A new Graphical scheme was introduced by Jansen [9, 10].This scheme had two phases one that is creation and the other is authentication .in the creation phase the user selects a theme that consist photos in a thumbnail size and a set of sequence of pictures as password. And then at the authentication phase the user has to recognize the images incorrect order. Each thumbnail is assigned a numeric value .Based on the thumbnails a numeric password is created. But the limit size of this password is 30.Hence Short password is created.

III. PROPOSED SYSTEM

General

First it will be checked that the user is already registered or not. If yes, then it will go for the step of login, but if user is not registered then first he will go through registration and then to the login step. Then at the time of transaction the color pairs and grid will be shown and from that the user will enter the session password. This password will be verified at the verification phase. If the user wants another session then a new session will be generated and the grid and color pair will be shown to the user again.

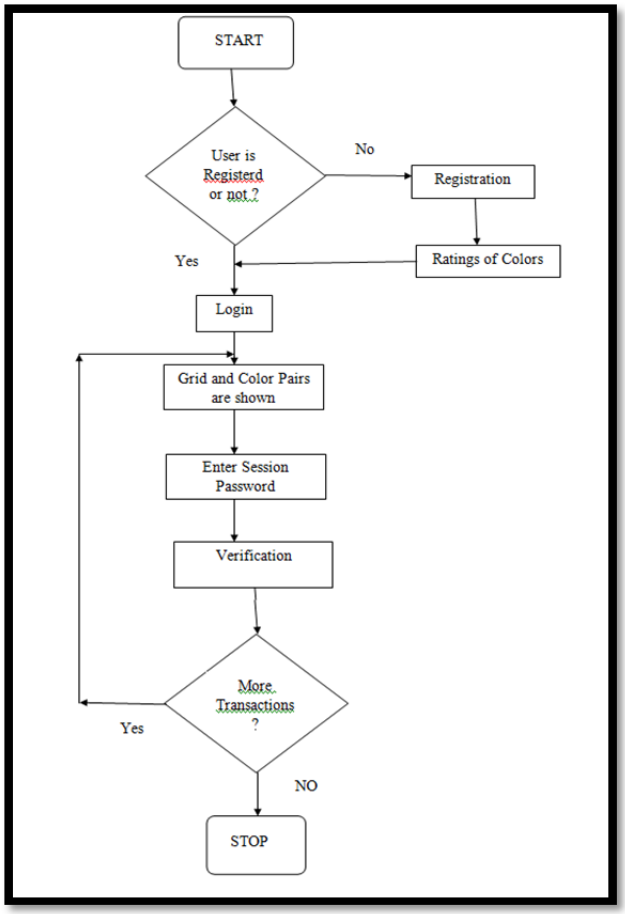

Fig. 5.a Working of Proposed system

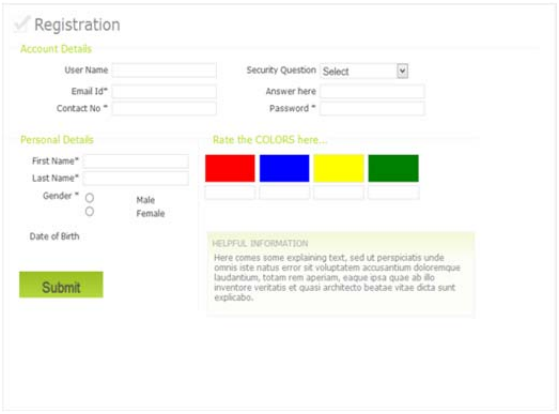

Fig .5.b Registration User interface

Authentication Scheme

1. During registration, user should rate colors as shown in figure 6. The User should rate colors from 0-9 and he can remember it as "BYGR". Same rating can be given to different colors.

Figure 6: Rating of colors by the user

2. 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 10x10. This grid contains digits 0-9 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 7. The color grid consists of 2 pairs of 4 colors. Each pair of color represents the row and the column of the grid.

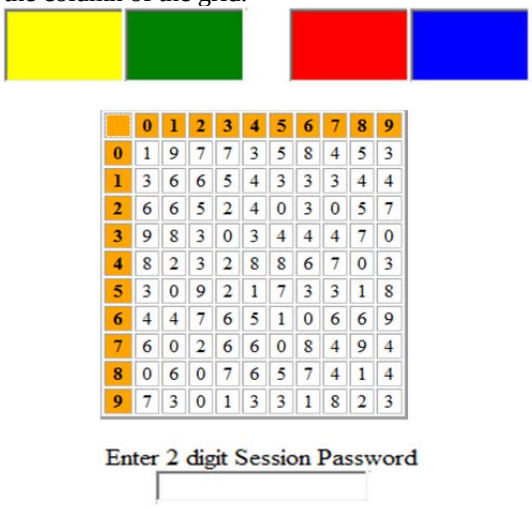

Figure 7: Login interface

Figure 7 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 6 ratings and figure 7 login interface for demonstration. Suppose the ratings for the figure 6 in BYGR format is given as 5362 at the time of registration. Now at the time of login after verifying the existence of username the user is expected to enter the session password .consider the figure 7 first pair has yellow and green colors. The yellow color rating is 3 and green color rating is 6. So the first letter of session password is 3rd row and 6th column intersecting element i.e. **4**. The same method is followed for pairs of red and blue. For figure 7 the password is **"40".** Instead of digits, alphabets can be also used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

Similarly we have implemented the system using 8 eight colors and correspondingly there will be 4 digit session password to be entered at the time of registration.

IV. 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 high complexity. So these are resistant to shoulder surfing attack.

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.

SQL injection Attack: Also in this proposed system the encryption of password stored in the database is done using rijn dael's algorithm, so in case if the attacker got access to the database the data is no longer useful unless it is decrypted by the code which present at the application side.

V. RIJN-DAEL'S ALGORITHM

Rijn dael (pronounced rain-dhal) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). [11]

The Rijn dael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. Rijn dael uses a variable number of rounds, depending on key/block sizes, as follows:

9 rounds if the key/block size is 128 bits
11 rounds if the key/block size is 192 bits
13 rounds if the key/block size is 256 bits

Also other asymmetric algorithm can be used for the purpose of encryption such as RSA algorithm but since it includes the concept of public and private key cryptography it makes the system very slow and rijn dael algorithm if used the efficiency of the system will much better.

VI. CONCLUSION

These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. This technique use grid for session passwords generation. 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 this scheme is completely new to the users and the proposed authentication techniques should be verified extensive.

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: Pass faces. 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. Sutra, 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.
[5] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.
[6] Passlogix, site http://www.passlogix.com.
[7] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing
[8] 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.
[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.
[10] W. Jansen, "Authenticating Users on Handheld Devices "in *Proceedings of Canadian Information Technology Security Symposium*, 2003.
[11] http://perso.uclouvain.be/fstandae/PUBLIS/11.pdf