ISSN:0975-9646

Authentication with Colours and Session Password

Priya More , Ankita Singh , Prakash Singh

Information Technology Department, Mumbai University
Xavier Institute of Engineering,Mahim,India

Information Technological Department
Xavier Institute of Engineering,Mahim,India

***Abstract*—In this paper we have specified about an authentication method which is all together different from existing technologies used for authenticating a system. Session passwords are passwords that will be used just once. Session password will be used in our technology which will provide a better security. Colors will used, user will give rating to color which will be used as his password. User just need to remember his colour rating. At time of authentication a grid with random numbers will be displayed along with colors appearing in pair on top of grid. In a pair of a colour 1st colour represent row and second the column. Based on the rating of colour that user gave user will find intersection of row and column and get the first digit of his session password. Similarly he will find the rest digit for password. Every time numbers in grid change and also the pairing of colour and so the password changes. This makes the system secure to great extent. This technology can be used in various field where data security is essential such as bank, military etc.**

***Keywords*—Session,colours rating,ASP.net,grid.**

I. 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.[4]

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 be added where the user can ask question about the working of the menus in website.

II. PROPOSED SYSTEM

The proposed system using new Authentication technique consists of 3 phases: registration phase, login phase and verification phase.There are two techniques that we are using to implement this project and those are Pair-based Authenticating Scheme and Hybrid Textual Authentication Scheme.

A. Pair-based Authenticating Scheme

During registration user submits his password. Maximum 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. 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.

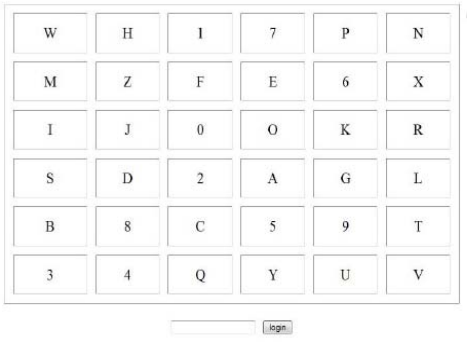
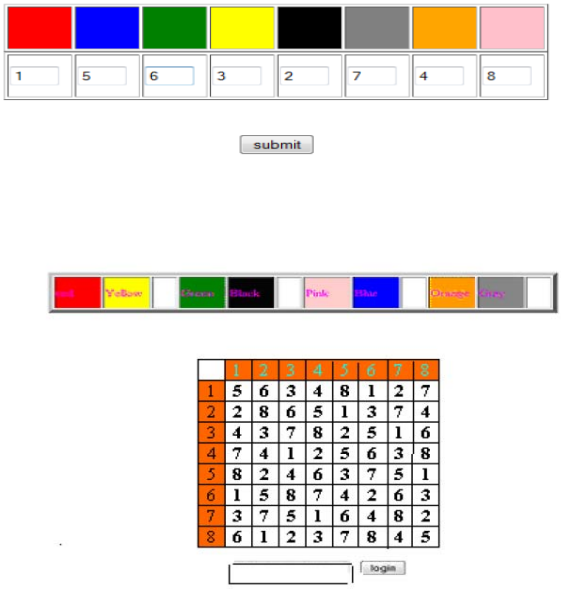


Fig.1 Pair based technique

B. *Using Hybrid Textual Authentication Scheme*

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. The color grid consists of 4 pairs of colors. Depending on the ratings given to colors, we get the session password.

Fig.2 Colour Rating



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Fig.3 Login interface

III. Scope

Textual password are very much vulnerable. Various attack are possible on them. System using session password provide much security. Authentication using color system can be used where security is very significant such as bank, army sector etc. we can use such system to protect the significant data.

IV. Conclusions

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

References

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9thUSENIX Security Symposium, 2000.

[2] [2]Z. Zheng, X. Liu, L. Yin, Z., (May 2010) “A Hybrid password authentication scheme based on shape and text” Journal of Computers, vol.5, no.5.

[3] [3]S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management”*.

[4] [4]Mr. Sagar A. Dhanake, Mr. Umesh M. Korade, Mr.Chetan P. Shitole, Mr. Sagar B. Kedar, Prof. V. M. Lomte, “*Authentication Scheme for Session Password using matrix Colour and Text*”.

[5] [5]M Sreelatha, M Sultan Ahamer, M Shashi , V Manoj Kumar , M Anirudh 1,“Authenticationv Schemes for Session PasswordsusingColor and Images”.