International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 03 | March -2019 e-ISSN: 2395-0126

Authentication Schemes for Session Passwords using Color and Images

1st Selva Priya R M.Sc.,(M.Phil) , 2nd Dharani S
1st Assistant Professor , 2nd UG Student
Department of Information and Computer Technology Sri Krishna Adithya College of Arts and Science
Bharathiar University of Coimbatore
Tamil Nadu –India
Email: selvapriyar@skacas.ac.in and dharanidharu9516@gmail.com

***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 the alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to the shoulder surfing. The text can be combined with the images and the 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, two techniques are proposed to generate the session passwords using the text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants. Therefore, we propose an authentication scheme using text and colors for generating session passwords.

***Keywords*—**Authentication session passwords, Pair-based Authentication Scheme, Hybrid Authentication scheme, Color PIN, Play-Fair Cipher, User Interface.

INTRODUCTION

Textual password is a very simple password scheme. It was used in the old days. The textual password is easily to trace so the system can access easily. Because user gives the passwords that are easy to remember, like pet name, date of birth, mobile number etc. So the textual password scheme as unreliable. For more security practices a new technology is invented that is Graphical password. It is very expensive system like a biometrics, thumb recognition, speech recognition, digital signature etc .But it was a very expensive so it is not affordable for user. Both the textual password and Graphical password having some drawbacks hence to remove such the drawbacks are newly security scheme is implemented or invented that is session password. It is very secure compares to remaining systems. Authentication technique consists of 3 phases:

registration phase, login phase and Verification phase. During registration, user enters his password in first method and 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. The most common technique used for authentication is textual password. The susceptibilities of this technique like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and long passwords can make the system as 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. Personal Digital Assistants is 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, new authentication schemes are proposed for PDAs. These schemes authenticate the user by session passwords. 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 the session passwords.

SECURITY ANALYSIS AND PERFORMANCE EVALUATION

Every time, the session password changes the interface also changes. This technique is resistant to shoulder surfing. Due to the dynamic passwords, dictionary attack is not applicable. In PDAs hidden camera attacks are not applicable because it is difficult to capture the interface in the Personal Digital Assistance.

Dictionary Attack:

This directly attacks towards on the textual passwords. In this type of attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems can access because the session passwords are used for every login.

Shoulder Surfing:

These techniques are Shoulder Surfing Resistant. Using Pair based scheme, resistance is provided by the fact that secret password created during registration phase and remains hidden so the session password cannot be enough to find secret pass in one session. In hybrid textual scheme, the randomized colors hide the password. The ratings of the session password decide in this scheme. But with

session password you can't find the ratings of colors. It is resistant to shoulder surfing even by knowing session password, the complexity is 84.

Brute force attack: These techniques are particularly resistant to brute force due to use of the session passwords. The use of these possibilities of the traditional brute force attack negligible.

Complexity: The Complexity for the Pair-Based Authentication Scheme is to be carried over the secret pass. The complexity is 368, for a secret pass of length 8. The complexity depends on the colors and ratings in the case of the Hybrid Textual Authentication Scheme. The complexity is 8 if ratings are the unique, otherwise it is 8.

EXISTING SYSTEM

The existing system to use the passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and the 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.

2.1 Biometrics

The biometric is one of the techniques for identification. It uses physiological or behavioral characteristics like retina scan, fingerprint scan as well as facial recognition or sound recognition to identify the user. But this technique is expensive.

2.2 Graphical password

The graphical password is most commonly used in authentication purpose. 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.

2.3 Digital signature

A digital signature is done by digital pen or any digital equipment. It is move to storage device by using some storing media. Once it is store in the database next time when login, the parameters can be check and if matching, the successfully login is granted.

The drawback of this technology is that an every user is not familiar with digital equipment. If you forget the parameter of signature then user cannot get the access to the system.

2.4Voice Recognition

Voice recognition refers to the recognition of human speech by computers and then performing a voice initiated program or function. The challenge that is handled so easily by the human brain, of interpreting speech amidst all accents, pitch, tone, articulation, nasality, vocalizations and pronunciation is a challenge when a computer tries to do it.

PROPOSED SYSTEM:

The proposed system using new Authentication technique consists of 3 phases: registration phase, login phase and 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.

Fig.1 Architecture of the proposed system

MODULES

1. **Pair-based Authentication scheme**
2. **Hybrid Textual Authentication Scheme**
3. **Registration Module**

3.1 Pair-based Authentication scheme Module:

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 password.

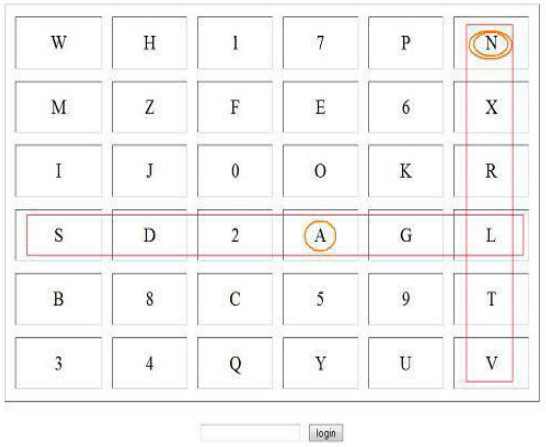

Fig.2 Intersection letter for the pair AN

3.2 Hybrid Textual Authentication Scheme Module:

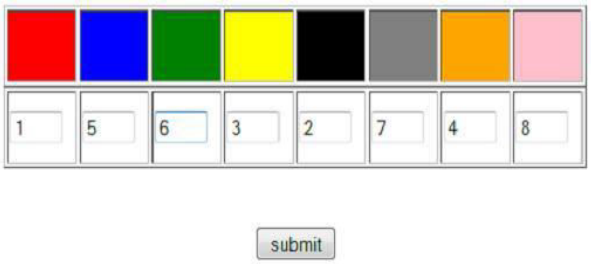

Fig.3: Color Rating

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.

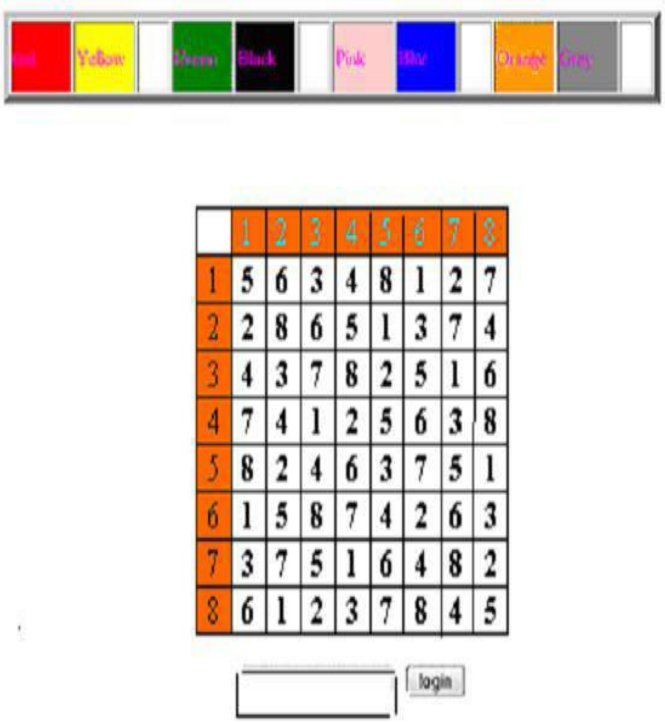

Fig.4: Color Rating Intersection Interface

3.3Registration Module:

This module is used to registered user Details in three parts. They are Name authentication password, Color Priority Password and Other details. First, user is going to enter the normal password but it using capital A-Z letters and 0-9 Numbers. Second the user to put the color priority in six colors.

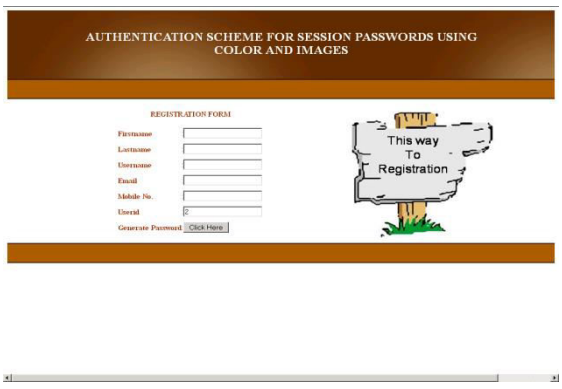

Fig.5: Regiration Form

Fig.6:Color Resitration

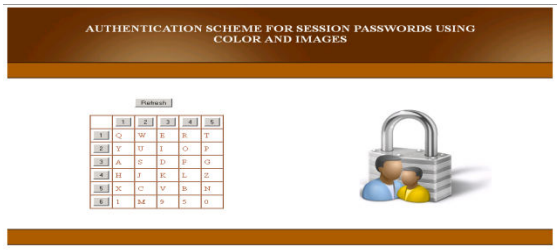

Fig.7:Image Registration

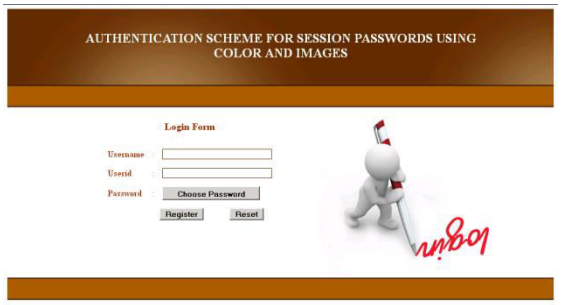

Fig.8: User Login

One Time Password Technique

This technique is used if the user wants to login through the Safe mode. Initially in the Safe mode, after the user authenticates the Pair based Authentication scheme, a code is sent to his/her mobile phone. This code has to be entered by the user in the next level of authentication. The code entered by the user is matched and the user is authenticated.

Registration

This module is used to register user details in three parts. They are namely Authentication Password, Color Priority Password and Other details. First, user is going to enter the normal password but it using capital A-Z letters and 0-9 Numbers. Second the user will put the color priority in eight colors.

SYSTEM SPECIFICATION

4.1 Hardware Requirements

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 14’ Colour Monitor.
- Mouse : Optical Mouse.
- Ram : 512 Mb.
- Keyboard : 101 Keyboards.

4.2 Software Requirements

- Operating system : Windows XP.
- Coding Language : PHP
- Data Base : MYSQL.

Future scope

It can be used in PDA's Folder locker or an external gateway authentication to connect the application to a database or an external embedded device. The proposed system is completely new to the users and should be verified extensively for the usability and effectiveness. This system can also be developed as windows application folder locker or as an external gateway authentication to connect the application to a database or an external embedded device.

Conclusion

More sites, more password, more forgetting, more repeated credentials. Increased exposure to hacking and cloning. It is more securable as compared to the existing system. It is not vulnerable so shoulder surfing, eves dropping and brute force attack.

REFERENCE

[1] 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.

[2] Haichang Gao, Zhongjie Ren, Xiuling Chang,Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant To Shoulder Surfing.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, "PassPoints: Design and longitudinal valuation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, **(2005)**, pp. 102-127.

[4] D. Weinshall, "Cognitive Authentication Schemes Safe against Spyware", (Short Paper), IEEE Symposium on Security and Privacy, **(2006)**.

[5] S. Chiasson, R. Biddle and P. C. van Oorschot, "A Second Look at the Usability of Click-based Graphical Passwords", ACM SOUPS, **(2007)**.

[6] L. F. Cranor and S. Garfinkel, "Security and Usability", O'Reilly Media, **(2005)**.

[7] R. N. Shepard, "Recognition memory for words, sentences, and pictures", Journal of Verbal Learning and Verbal Behavior, vol. 6, **(1967)**, pp. 156-163.

[8] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security", in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, **(1999)**.

[9] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall", in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, **(2004)**, pp. 1399-1402.