Secure Hybrid and Pair-Based Password Authentication Scheme

Miss. Raut Manisha S[1] Miss. Lokhande Dipeeka S[2] Miss. Antre Ashwini P[3]
Miss. Musale Pradnya S[4]
[4]HOD
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]S.C.S.C.O.E., Rahuri Factory

Abstract— As the increase in the amount of personal information in electronic forms, there is a need for securing this information. Alphanumerical or textual username and password (combination of text or number) is most common method of authentication, but these passwords are vulnerable to different attack like shoulder surfing, dictionary attack, password guessing etc. Later graphical passwords are come into existence, but the drawback of this is, it takes more time for authentication. To overcome these problems, we introduced new authentication scheme which is session password. In this we used a pair –based methods. In pair-based scheme we use textual password for authentication.

Key words: Session password, OTP, Pair-based authentication

I. INTRODUCTION

Authentication is any process or set of rules that permits one entity to institute the identity of another entity, so in order to protect user account the authentication must be secured. The textual password is a common method which we used earlier, in which the lengthy password is considered as a secure password, but they are difficult to remember. Thus user picks short password but they are easily cracked or hacked.

Later the new technique graphical password is proposed, this technique overcome the shoulder surfing problem in the textual password but it has its own limitations like it take more time for authentication and it is quite expensive.

Thus in this paper we proposed a new password authentication scheme which use session password. The new scheme is introduce which is Hybrid (color-code) and Pair-Based Textual Authentication Scheme. When user login into system new session is generated and it remains until user gets logout. System generates new password for every new session and it valid only for this session. When session terminated this password is no longer responding. These techniques provide more security as it create new password for every session.

II. LITERATURE SURVEY

Set M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar, "Authentication Schemes for Session Passwords using Color and Images". Common method used for the authentication, is Textual passwords. But textual passwords are vulnerable to distinct attacks like eves dropping, password guessing, dictionary attacks, social engineering and shoulder surfing. As alternative techniques to textual passwords the Graphical passwords are introduced. Most of the graphical schemes are victim to shoulder surfing. To overcome this problem, text can be combined with colors or images to generate session passwords for the authentication. Session password is a password that can be used only once and for each time a new password is generated. In this paper, the techniques are proposed to generate session passwords using color and text which are resistant to shoulder surfing. These two methods are suitable for Personal Digital Assistants (PDA) [2].

Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, "The design and analysis of graphical passwords". The paper evaluate new password technique that is graphical password, to achieve better security than text based passwords exploit features of graphical input displays. Graphical input devices enable the user to decouple the location of inputs from the order in which those inputs occur and we show that this decoupling can be used to generate password schemes with considerably larger password spaces. In order to evaluate the security of one of schemes, it plan a novel way to gain control of a subset of the memorable passwords that, we believe, is itself a contribution. In this work we are essentially motivated by devices such as PDAs (personal digital assistants) that offer graphical input abilities via a stylus, and we describe our prototype accomplishes one of our password schemes on such a PDA, namely the Palm Pilot[3].

R. Dhamija, and A. Perrig "A User Study Using Images for Authentication". Now secure systems suffer from attacks because they ignore the human factor's importance in security. We address a basic weakness of knowledge-based authentication technique, which is limitation of human to remember secure passwords. Our work is begin to improve the security of these systems relies on recognition-based, rather than recall-based authentication. We inspect the requirements of a recognition-based authentication system and in propose D'ej'a Vu, which authenticates a user through her ability to recognize previously seen images. D'ej'a Vu is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall PINs or passwords. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to share or write down passwords with others [4].

Robert Biddle, Sonia Chiasson P.C. Van Oorschot"Graphical Passwords: Learning from the First Twelve Years" Many graphical scheme have been proposed as alternatives to text- based password authentication. This paper provide overview of published researches, covering both usability and security aspect. The paper first catalogues existing approaches, highlight novel features of selected schemes and identify key usability or advantages of security. For knowledge-based authentication it then review usability requirements as they apply to graphical passwords, identify security threats that such system must address and review known attacks, empirical evaluation issues are discuss and

identify areas for further research and improved methodology.[5]

III. PROPOSED SYSTEM

Currently for authentication alphanumerical (text or number) username and password is used basically so to prevent hackers from accessing the account data, the security must be provided. The authentication is provided by using hybrid and pair-base scheme. In pair-based scheme the textual passwords are provided and in hybrid scheme the color-code is provided.

Authentication technique consists following phases:

1) Registration phase
2) Login phase
3) Verification phase

A. Registration Phase

In registration phase user enter his/her Personal information like Address, Mobile number, Username, Password etc.

B. Login Phase

During login phase based on the interface displayed on the screen, user has to put the password. User have to make pairs of his/her password's letters or digits. After pressing each word in the password, the interface get changed. The virtual keyboard algorithm is used for changing interface.

This algorithm work as follow:-

1) Initialize the all keyboard buttons in the QWERTY pattern.
2) While the key is pressed,
   a) Stored all numbers and alphabates in the array.
   b) Randomize the all numbers and alphabates.
   c) Reassign the newly formed alphabates and number to the buttons in the array.
   d) Display the characters on the buttons.
   e) If enter key is pressed go to step 3.
3) Check the length of the keys entered in the database. If (length = valid)
4) Check for the password match.
   a) If password match go to step 6.
   b) Else go to step 5.
5) Second level of authentication.
6) End.

C. Verification Phase

The system verifies entered password by comparing it with the content of password which is generated at the time of registration. If password is matched user allow to login system. If not then user should try again.

IV. SYSTEM ARCHITECTURE

At the time of login user first enter his/her username, after that enter password. User can choose one of the method from hybrid and pair-based scheme at the time of registration. At the time of entering password select that method which we used at the time of registration and user have to make pair of his/her password's letters for generating session password. First letter of pair is used to select row and second is for column. The letter which is at the location of the intersection of that row and column is the session password. User have to enter this intersection letter for login.

For pair-based method if length of registered password is 8(even) then session password has length 4, because it is obtaining by making pair of letters in original password. When length of registered password is 7(odd) then session password has length 4, it make pair of letters in original password and last letter enter as it is, because there is no letter to make pair with that letter.

For hybrid method the length of password is eight. Because, in proposed system we used eight colors.

When user enter username system itself generate session password as a OTP and send it to user's mail. So user can get that OTP from mail and without generating session password directly login by entering OTP.

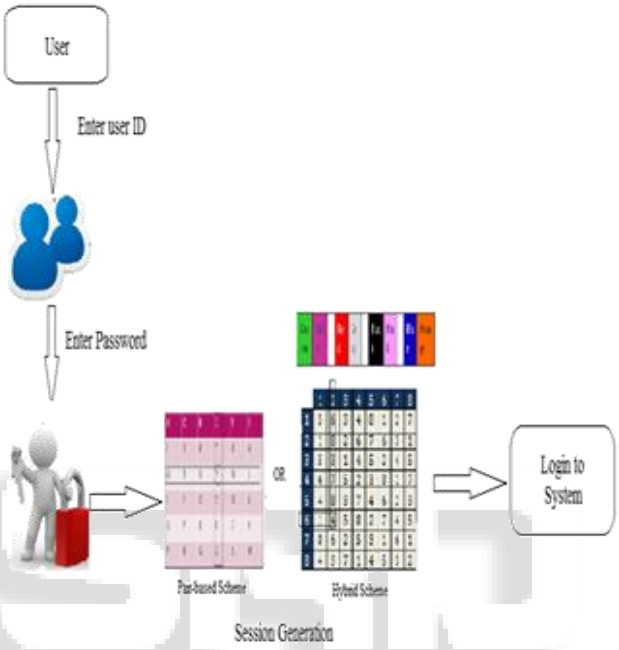

Fig. 1: System Framework

A. Hybrid-Based Authentication Scheme

In this method with the help of colors user get password. During registration, user have to fill his/her information and rate the colors. At the time of registration user should rate colors from 0 to 7or 1 to 8 according to his/her opinion.

The login interface consists of 8*8 grids.During Login the colors selected by the user is display on the login page in pairs.As it has 8 colors the color grid consists 4 pairs of colors. In each pair first color represent row and second color represent column.

Fig. 2: Rating of colors by the user

The intersection of row and column is taken and the digit on that intersection is inserted in the password field.

Consider an example, suppose at the time of registration user rate color as shown in above fig. 2. Then session password generated is as follows:

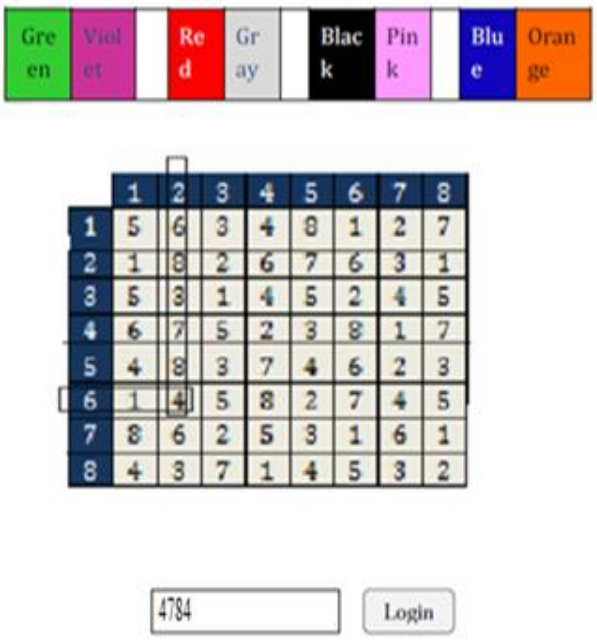

Fig. 3: Login Interface

In above fig. the first pairs have green and violet colors. The rating of green is 6 and violet is 3. Green colors is selected as row and violet as column. Their intersection is taken which is 4 which is a session password and is inserted into password field.

This process is repeated for remaining color pairs in the color grid. The generated password 4784 is inserted into password field for login to the system.

B. Pair-Based Textual Authentication Scheme

In pair-based authentication scheme, user submit his/her password at the time of registration. The maximum length of password is eight. When the user enters login an interface consisting of grid of size 6*6 and it contain alphabets and numbers. These are randomly placed on the grid and interface change every time

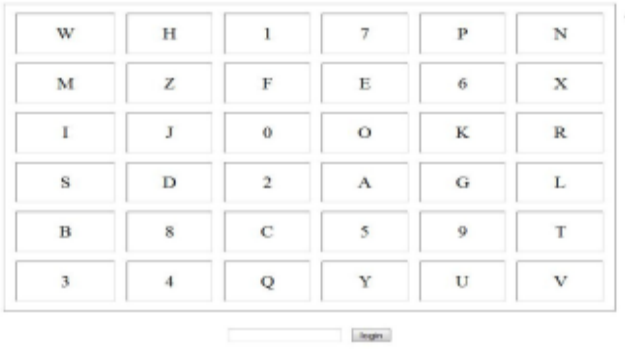

Fig. 4: Login interface

User have to consider his/her password in terms of pair. Now the user have to enter his/her authentic password which is intersection part of that submitted password.

Suppose we submit the password during registration as a "ADMIN456" in which 4 pairs taken into password. The first letter in the pair is used to select the row and second letter is used to select the column. This is repeated for all pairs of submitted password.

Fig. 5: Intersection letter for the passwords pair ADMIN456

The above fig. show the intersection of password pair "AD" is letter 2. Similarly for the intersection of password pair "MI" is letter M, for the intersection of password pair "N4" is letter K, for the intersection of password pair "45" is letter L, so this four inter- section letters "2MKL" is the session.

C. OTP (One Time Password)

The password which is valid for only one session is called OTP. The OTP is used when user wants to login through the safe mode. In safe mode after user authentication the pair-based authentication scheme the code is send to the user mail. It is no longer valid after session termination. This OTP is compared by the code and when code matched user is authenticated.

V. EXPERIMENTAL RESULT

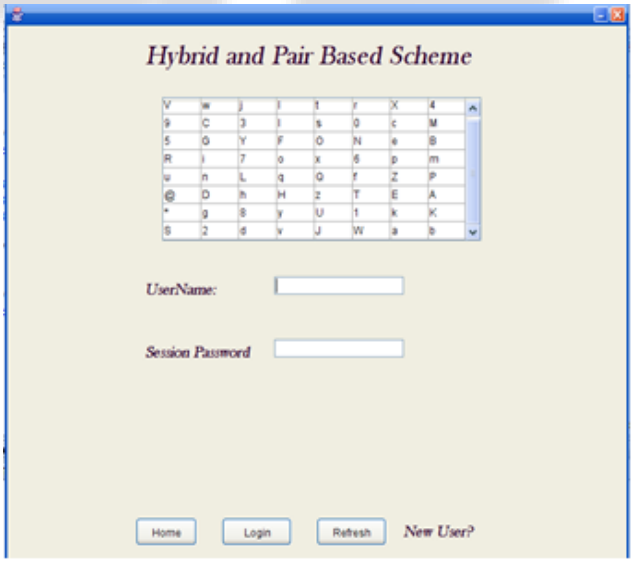

Fig. 1: Hybrid Scheme

In pair-based authentication scheme, user submit his/her password at the time of registration. The maximum length of password is eight.

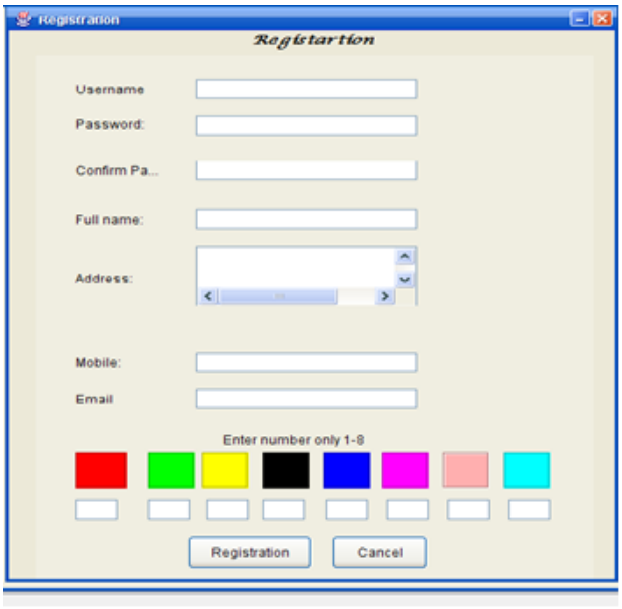

Fig. 2: Registration Register details with all mandatory fields

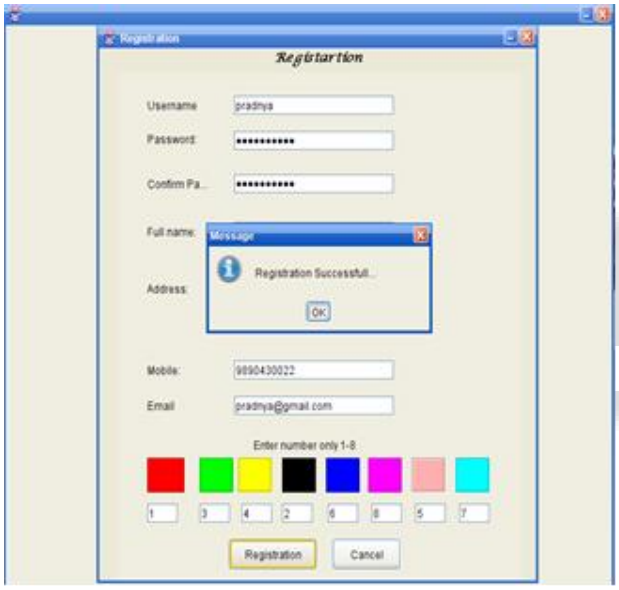

Fig. 3: Registration After the successfully login system can send OTP password to valid login

Fig. 4: Hybrid paired based scheme The OTP is used when user wants to login through the safe mode

VI. Conclusion

The proposed scheme allow user to login through new modes hybrid and pair-based technique. In these techniques new password for each session is provided. In this scheme password provides more security than the existing system because for every session new session password is generated.

References

[1] Reshma Dilip Kadam computer KJCOEMR pune, Maharashtra. ”Authentication schemes for session password using hybrid and pair based Techniques”. Multidisciplinary Journal of research engineering and technology 2014.

[2] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar “Authentication Schemes for Session Passwords using Color and Images”, International Journal of Network Security & Its Applications (IJNSA), May2011.

[3] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing.

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

[5] Robert Biddle, Sonia Chiasson , P.C. van Oorschot, “Graphical Passwords:Learning from the First Twelve Year”2000.

