Authentication Scheme For Session Password Using Play-Fair Cipher

Vishal Janjalkar[1], Shekhar Mulik[2], Archana Nanade[3]
UG Students [1] & [2], Professor[3]
Department of Information Technology
Theem College of Engineering, Boisar
University of Mumbai
Maharashtra – India

Abstract— **Classical PIN entry mechanism is extensively intended for authenticating a user which stabilizes the usability and security fragments of a system. However, if this scheme is to be used in a public system then the scheme may struggle with shoulder surfing attack. In which, an abandoned user can fully or partially observe the login session. Even the events of the login session can be recorded so that invader can use it later to get the actual PIN. Textual passwords are the most usual method used for authentication however they are defenceless to dictionary attacks, social engineering and various snooping attacks. Graphical passwords are alternate techniques to textual passwords. As most of the graphical schemes are defenceless to shoulder surfing. To point this problem, text can be joint with images or colors to produce session passwords for authentication Session passwords could be used once and each time a new password is generated. Here two procedures are projected to generate session passwords using text and colors which are unaffected to shoulder surfing. These approaches are appropriate for Personal Digital Assistants. However, one huge concern sustained with the GUA is that it is very exposed to shoulder-surfing and spyware attacks. Here, we use Play-Fair Cipher that could restrict or filibuster shoulder-surfing and spyware attacks. This scheme uses an algorithm called as Play-Fair Cipher which is a digraph substitution cipher.**

Keywords—**Color PIN, Play-Fair Cipher, User Interface, Authentication, session passwords, pair-based authentication scheme, hybrid textual authentication scheme.**

I. INTRODUCTION

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 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. 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, 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.

II. EXISTING SYSTEM

The existing system to use 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.

A. Characteristic of user chosen PIN

In the conventional schemes it is required to remember either few digits or few characters as user PIN. But in our scheme the color is used to form a PIN. User can choose four colors from a set of ten different colors represented as {C0, C2, C3, C4}. So one possible instance of user chosen PIN might be C1C2C3C4. Each Ci denotes a specific color (say yellow or brown). As user chosen PIN is comprised of four colors so probability of guessing the PIN will be 1/104.

ISSN: 2278 – 1323

B. *Steps of Login Procedure*

In this subsection we will discuss about how user will interact with system during entire session.

• User enters his login id.

• Once system checks that the login id exists then it will generate Feature Tables.

• System then generates four random challenge values ranges from 1⋯10.

• Next user will have to give response to those challenge values (User response ranges from 0 to 9).

• User response will be evaluated by system.

• Finally system will decide whether the user is legitimate or not.

User interface for login has been given in Section IV. Algorithms used in the above procedure, have been described in Section III-E.

C. *Characteristic of Feature Tables*

Color Pass interface consists of 10 different Feature Tables which are numbered from 1 to 10. Each cell of a table is represented by a pair <C i, V i>. Here Ci denotes the color of the cell i and Vi indicates the digit corresponding to cell i. Ci is unique with respect to a Feature Table. Thus no color occupies in more than one cell. So for a particular table there will be ten different color cells. The positions of color cells is shown in Table I and this is fixed for every table. So if first cell of a table is filled with C1 then first cell of all other tables are also filled with C1.

	0	
1	2	3
4	5	6
7	8	9
	K	

TABLE I: Identifying Each Cells in k^{th} table

All cells in a table also contain a unique value Vi from the set {0, 1,...,9}. Another important characteristics is that in each cell i, the pair <C i,Vi> is unique with respect to all the cells in all the ten tables. Thus if first cell of First Feature Table contains <C 1,0 > then first cell of any other Feature Table will not contain <C 1,0 >. The orientation of these colors and digits in those cells are also fixed for every session. The numbers written in bold denotes the table number of each Feature Table. The empty cells in the tables denote nothing.

I. PROPOSED SYSTEM

The proposed system using new Authentication technique consists of 3 phases:

1) Registration Phase
2) Login Phase
3) Verification Phase

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.

A. *Proposed Algorithm*

One of the techniques involve a 6*6 alphanumeric matrix while the other includes a color palette along with a numeric matrix that are unlocked using the concepts of play fair cipher cryptographic method for the high rate of security in applications.

This project investigates a cipher that is somewhat more complicated than the simple substitution cipher. The **Play-Fair cipher** is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Play fair who promoted the use of the cipher.

The technique encrypts pairs of letters (*digraphs*), instead of single letters as in the simple substitution cipher and rather more complex. The Play fair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. The frequency analysis of digraphs is possible, but considerably more difficult. We used A-Z 26 letters and 0-9 digits for 6*6 grid matrix to encrypt the password.

A B C D E
F G H I K
L M N O P
Q R S T U
V W X Y Z

To encode a message, one breaks it into two-letter chunks. Repeated letters in the same chunk are usually separated by an X. The message, "HELLO ONE AND ALL" would become "HE LX LO ON EA ND AL LX". Since there was not an even number of letters in the message, it was padded with a spare X. Next, you take your letter pairs and look at their positions in the grid.

"HE" forms two corners of a rectangle. The other letters in the rectangle are C and K. You start with the H and slide over to underneath the E and write down K. Similarly, you take the E and slide over to the H column to get C. So, the first two letters are "KC". "LX" becomes "NV" in the same way.

"LO" are in the same row. In this instance, you just slide the characters one position to the right, resulting in "MP". The same happens for "ON", resulting in "PO". "EA" becomes

ISSN: 2278 – 1323

"AB" in the same way, but the E is at the far edge. By shifting one position right, we scroll around back to the left side and get A.

"ND" are in a rectangle form and becomes "OC". "AL" are both in the same column, so we just move down one spot. "AL" is changed into "FQ". "LX" is another rectangle and is encoded as "NV".

The resulting message is now "KC NV MP PO AB OC FQ NV" or "KCNVMPPOABOCFQNV" if you remove the spaces.

This encoder will do all of the lookups for you, but you still need to do a few things yourself.

1. Manually break apart double letters with X (or any other) characters. Some people break apart all doubles, others break all doubles that happen in the same two-letter chunk. This encoder requires neither in order to be more flexible.

2. Manually make the message length even by adding an X or whatever letter you want. If you don't, the encoder will automatically add an X for you.

All non-letters are ignored and not encoded. The one letter that you select to share a square in the cipher is translated. Numbers, spaces, and punctuation are also skipped. If you leave two letters together in a two-letter chunk, they will be encoded by moving down and right one square ("LL" becomes "RR") where as traditional Play-Fair Ciphers will automatically insert an X for you.

B. Advantage

1. The Session passwords are passwords that are used only once.

2. The users input different passwords.

3. The session passwords provide better security against dictionary and brute force attacks as password changes for every session.

C. System Architecture and Explanation

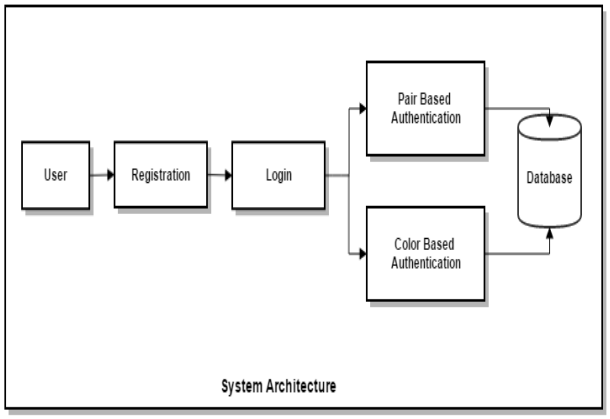

Fig. 1 System Architecture

Fig. 1 shows that architecture of system.

1. User will register his details with text password and give ranking to colors.
2. At the time of login User has to enter his username and password.
3. Here we have to choose password as intersection of rows and columns of pairs of the passwords.
4. And then give the same rating to the colors as given in registration time.
5. System will authenticate the user, if details are correct, Login successful else login failed.

D. MODULES

1. Pair-based Authentication scheme

2. Hybrid Textual Authentication Scheme

3. Registration

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 pass.

ISSN: 2278 – 1323

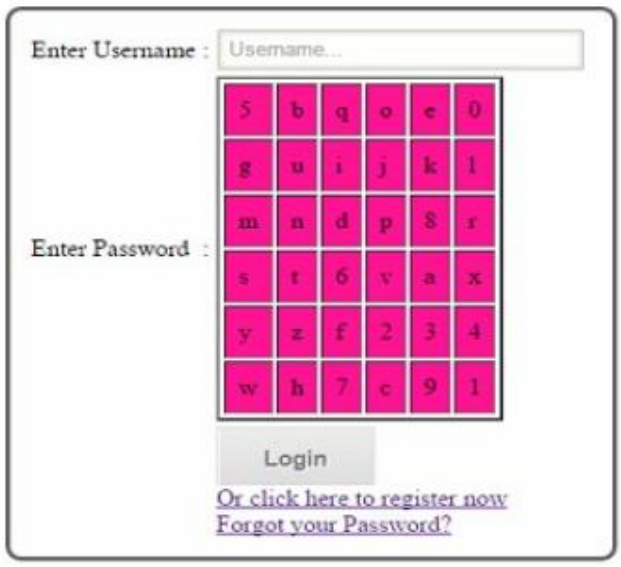

Fig.2. Pair-based authentication

Hybrid Textual Authentication Scheme Module:

The User should rate colors from 1 to 6 and he can remember it as "RBBPGG". Same rating cannot 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 interface contains strips of colors. The color strip consists of 6 colors. Depending on the ratings given to colors, we get the session password.

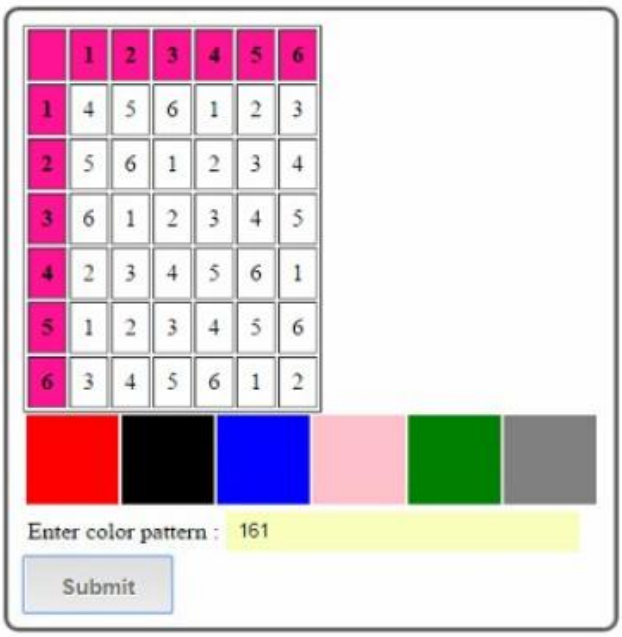

Fig.2. color-codes authentication

Registration 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.

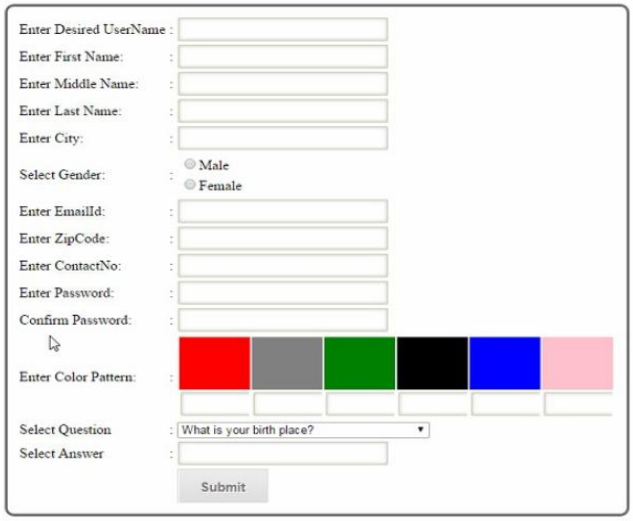

Fig.3. Registration Form

II. CONCLUSION

These password techniques are an alternative to textual alphanumeric password. Because of session password, it is hard to guess. It is more securable as compared to the existing system. It is not vulnerable to shoulder surfing, eves dropping and brute force attack. 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] Nilesh Chakraborty, Samrat Mondal, "Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack." IEEE-2014.

[2] Narayan Gowraj, Srinivas Avireddy, "SAFE: Shoulder-Surfing Attack Filibustered With Ease." IEEE-2013.

[3] Song Luo, Jianbin Hu, Zhong Chen "An Identity-Based One-Time Password Scheme with Anonymous Authentication." IEEE-2009

[4] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. D. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Man-Machine Studies, vol. 63, no. 12, pp. 102–127, 2005.

[5] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," International Journal of Network Security, vol. 7, no. 2, pp. 273–292, 2008.

[6] T. Perkovic, M.C″ agalj, and N.Saxena, "Shouldr-surfing safe login in a partially observable attacker

ISSN: 2278 – 1323

model," in Sion, R.(eds.) FC 2010. LNCS, pp. 351–358, 2010

[7] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM Journal on Computing, vol. 15, pp. 364–383, may 1986.

[8] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu,"A New Graphical Password Scheme Resistant to Shoulder-Surfing" 2010 International Conference on Cyberworlds.

[9] C. Herley, P. C. Oorschot, and A. S. Patrick, "Passwords: If were so smart, why are we still using them?" in Financial Cryptography, pp. 230–237, 2009.

ISSN: 2278 – 1323