www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 6 June 2016, Page No. 16785-16791

Intelligent Techniques with GUI by Challenge Keypad for Secure Password

Mr. Krishna S. Gaikwad, Prof. Amruta Amune
Department of Computer Engineering
G.H.Raisoni College of Engineering and Management, Ahmednagar.
Email- gaikwadkrish91@gmail.com

Abstract—In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. This problem has come up with a new solution. Devising a user authentication scheme based on personal identification numbers (PINs) that is both secure and practically usable is a challenging problem. The greatest difficulty lies with the susceptibility of the PIN entry process to direct observational attacks, such as human shoulder-surfing and camera-based recording. PIN entry mechanism is widely used for authenticating a user. It is a popular scheme because it nicely balances the usability and security aspects of a system. However, if this scheme is to be used in a public system then the scheme may suffer from shoulder surfing attack. In this attack, an unauthorized user can fully or partially observe the login session. Even the activities of the login session can be recorded which the attacker can use it later to get the actual PIN. In this paper, we propose an intelligent user interface, known as Color Pass to resist the shoulder surfing attack so that any genuine user can enter the session PIN without disclosing the actual PIN. The Color Pass is based on a partially observable attacker model. The experimental analysis shows that the Color Pass interface is safe and easy to use even for novice users.

Index Terms—PIN, Shoulder Surfing Attack, User Interface, Partially Observable.

I. INTRODUCTION

In a recent,the number of Internet users has been reported as approximately 2.4 billion worldwide, and from 2000 to 2012, it is a staggering 566.4Percentage increase. This huge number of users consists of both genuine users and malicious users. So software applications which deal with sensitive and private information, must provide a sound protection to the system so that genuine and malicious users can be identified properly. In computer security, authentication is such a technique by which the system identifies the genuine users. Among several authentication schemes, password based authentication is still one of the widely accepted solution for its ease of use and cost effectiveness [1] and we can use with our smart knowledge basis[2]. Though conventional PIN entry mechanism is widely famous for ease of usability, but it is prone to shoulder surfing attack [3] in which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN.

The different methods are graphical passwords and biometrics. On the other hand these methods have their particular disadvantages. In Biometrics password techniques such as facial recognition, finger prints etc. have been presented but not yet commonly adopted. The main disadvantage of this method is that such systems can be costly and the identification procedure can be slow. There are numerous graphical password methods that are planned in the past years. On the other hand most methods are suffer from shoulder surfing attack which is becoming somewhat a large problem. There are graphical passwords patterns that have been projected which are resistant to shoulder-surfing on the other hand they have their particular weaknesses like usability problems or takes more time for login or it has tolerance levels. The shoulder surfing attack in an attack that can be did by the opponent to get the users password by observing above the users shoulder as he enters his password. From the time numerous graphical password methods with different degrees of resistance to shoulder surfing has projected, e.g.,Shoulder-surfing resistant graphical password[4],Images Authentication[5],Evaluation in Shoulder surfing password[6],Evaluation in Shoulder surfing password [7],Graphical password Schemes [8],Replacement of Alpha Numeric password[9],Shoulder surfing password scheme[10],Shoulder surfing safe login[11] and each has its pros and cons. As predictable password schemes are susceptible to shoulder surfing, Sobrado and Birget [4] proposed three shoulder surfing resistant graphical password methods.

Seeing that maximum users are more used text-based passwords than graphical passwords, Zhao et al. [12] proposed a text-based shoulder surfing resistant graphical password methods, S3APS. In S3PAS, the user has to fusion his textual password on the login screen to catch the session password. However, the login procedure of Zhao et al.s methods is difficult and boring. And then, a number of text-based shoulder surfing resistant graphical password methods have been proposed, such as Shoulder surfing password-image based authentication[13],Salable Shoulder surfing password textual authentication scheme[14],Login Record attack-sector login[15],session password using color and images[16],Shoulder surfing password for mobile environment[17].

Based on the information available to the attacker, secure login methods can be classified into two broad categories fully observable and partially observable. In the first one, the attacker can fully observe the entire login procedure for a particular session and in the second one, the attacker can partially observe the login procedure. Our proposed

methodology falls into second category and users are required to remember four colors instead of conventional four digit PINs. The proposed Color Pass methodology implements onetime pass paradigm. Thus corresponding to four color PINs, the user gets four challenges and enters four responses with respect to each challenge. The main objective of Color Pass scheme is that it is easy to use and does not require any special prerequisite knowledge. In addition to the resistance against shoulder surfing attack, it also provides equal password strength as compared with the conventional PIN entry scheme.

II. RELATED WORKS

Perrig and Dhamija [5] proposed a graphical authentication methods where the user has to recognize the pre-defined images to verify users authenticity. In this scheme, the user chooses a number of images from a group of random images during registration. After, during login the user has to recognize the previously selected images for authentication from a group of images as shown in figure 1. This methods is vulnerable to shoulder-surfing. In 2002, Sobrado and Birget [6] proposed three shoulder surfing resistant graphical password schemes, the Intersection methods, the Movable Frame methods, and the Triangle methods. However, both the Movable Frame methods and the Intersection methods have high failure rate. In the triangle methods, the user has to choose and remember more than a few pass-icons as his password. To login the system, the user has to properly pass the predetermined number of challenges. In every challenge, the user has to find three pass-icons among a set of randomly selected icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons.

Wiedenbeck et al. [7] proposed in 2006, the Convex

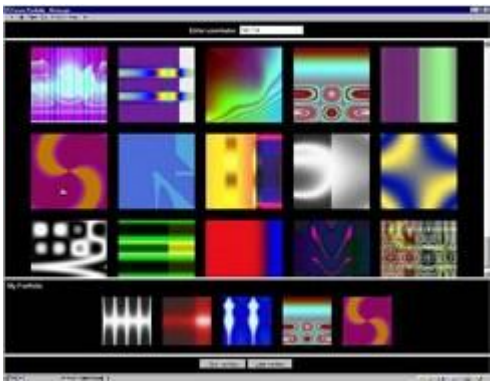


Fig. 1. images used by Dhamija and Perrig

Hull Click Scheme (CHC) as a better version of the Triangle scheme with greater security and usability. To login the system, the user has to properly respond some challenges. In each challenge, the user has to find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull designed by all the showed passicons. But, the login time of Convex-Hull Click scheme may be too long. In 2009, Gao et al. [8] proposed a shoulder surfing resistant graphical password scheme, Color Login, in which the background color is a usable issue for decreasing the login time. Still, the possibility of accidental login of Color Login is too high and the password space is too small. In 2009, Yamamoto et al. [13] proposed a shoulder surfing resistant graphical password scheme, TIIBA, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for the user to find his pass-icons. Unluckily, TIIBAs resistance to accidental login is not strong. And, it may be problematic for some users to find his pass-icons temporally displayed on the login display.

As maximum users are aware with word-based passwords and conventional text-based password authentication schemes have no shoulder surfing resistance. In 2007, Zhao et al. [14] proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to discover his textual password and then follow a special rule to mix his textual password to catch a session password to login the system. On the other hand, the login procedure of Zhao et al.s methods is difficult and boring. Sreelatha et al. [16], in 2011, also proposed a textbased shoulder surfing resistant graphical password scheme by using colors. Clearly, as the user has to in addition remember the order of some colors, the memory load of the user is high. In the similar year, Kim et al. [17] proposed a text based shoulder surfing resistant graphical password scheme, and employed an analysis method for accidental login resistance and shoulder surfing resistance to analyze the security of their scheme. Unluckily, the resistance of Kim et al.s scheme to accidental login is not acceptable, suggested a text-based shoulder surfing resistant graphical password scheme, PPC. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four predefined rules to get his session password on the login screen. On the other hand, the login procedure of PPC is too complex and boring.

User should rate colors during registration as shown in figure 2. The User should rate colors from 1 to 8 and he can recall it as RLYOBGIP. Identical rating can be given to dissimilar colors. During the login phase, when the user write or enter his username a one interface is showed based on the colors designated by the user. The login interface consists of grid of size 88. This grid encloses digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. The color grid contains of four pairs of colors. Each pair of color denotes the row and the column of the grid.

Haichang et al [18] proposed a shoulder-surfing resistant scheme where the user is essential to draw a curve through their password images orderly rather than ticking on them directly. This graphical method combines Story and DAS method to deliver authenticity to the user. Syukri [19] proposed a methods where authentication is done by sketch user signature using a mouse.This technique involved two phases, verification and registration. At the time of

DOI: 10.18535/ijecs/v5i6.10

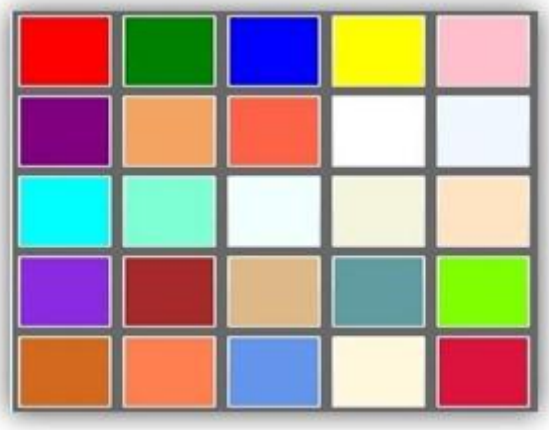


Fig. 2. images used by Dhamija and Perrig

registration phase the user draws his signature with the help of mouse, afterward that the system extracts the signature zone. Then in verification phase takings the user signature as input and fixes the standardization and then excerpts the parameters of the signature. The drawback of this method is the forgery of the signatures. Is not shoulder surfing resistance.

III. THE PROPOSED SCHEME

The proposed Color Pass interface is based on partially observable attacker model in which an attacker cannot see the challenge values generated by the system but can only see the response given by the user. Thus it is assumed that the media through which user gets the challenge should ensure security against man-in-middle attack [20]. In this section we first discuss about the characteristic of user chosen PIN followed by user login procedure for a session. Then we give details about the structure and characteristics of tables used in implementing Color Pass. And then we discuss about PIN entry mechanism using our proposed methodology.

A. 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,,C9. User has the flexibility to choose one color more than once. So one possible instance of user chosen PIN might be C1C2C1C4. Each Ci denotes a specific color (say yellow or brown).

B. Login Procedure

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

1.User enters his login id.

2.Once system checks that the login id exists then it will generate Feature Tables using Algorithm 1.

3.System then generates four random challenge values ranges from 110.

4.Next user will have to give response to those challenge values (User response ranges from 0 to 9). 5.User response will evaluated by system using Algorithm 2.

6.Finally system will decide whether the user is legitimate or not using Algorithm 3.

C. 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 ¡ Ci,Vi ¿. 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 III 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 ¡ Ci,Vi ¿ is unique with respect to all the cells in all the ten tables. Thus if first cell of First Feature Table contains ¡ C1,0 ¿ then first cell of any other Feature Table will not contain ¡ C1,0 ¿. The orientation of these colors and digits in those cells are also fixed for every session. All the ten Feature Tables are shown in Table IV to Table XIII. The numbers written in bold denotes the table number of each Feature Table. The empty cells in the tables denote nothing.

D. Algorithm for Generating Tables

Suppose ten different colors C0, C2,...,C9 are stored in an array Color[] (index ranges from 0 to 9). This array is required as an input to the Algorithm 1. Now lets assume that each Feature Table is denoted as FT(i) and each cell is represented by CELL(j). So to refer a cell of a table we use the operator FT(i).CELL(j). Now each cell has two dimensions - Color and Value. So to access the color of 5th cell of 8th Feature Table, we can use the following notation

DOI: 10.18535/ijecs/v5i6.10

FT(7).CELL(4).Color

and to access the corresponding value we have to use the following

FT(7).CELL(4).Value

Algorithm 1-Generating tables in Color Pass Input: This algorithm will take array Color [0,1,...9] as input. Output: It will generate Feature Tables FT(0)FT(9) for i = 0 to 9 do for j = 0 to 9 do

FT(i).CELL(j).Color Color[j]
FT(i).CELL(j).Value (i+j) mod 10; end for end for

	$C_1(0)$	
$C_1(1)$	$C_1(2)$	$C_1(3)$
$C_1(4)$	$C_1(5)$	$C_1(6)$
$C_1(7)$	$C_1(8)$	$C_1(9)$
	1	

TABLE II: First feature table of Color Pass

	$C_1(1)$	
$C_1(2)$	$C_1(3)$	$C_1(4)$
$C_1(5)$	$C_1(6)$	$C_1(7)$
$C_1(8)$	$C_1(9)$	$C_1(0)$
	2	

TABLE III: Second feature table Of Color Pass

	$C_1(2)$	
$C_1(3)$	$C_1(4)$	$C_1(5)$
$C_1(6)$	$C_1(7)$	$C_1(8)$
$C_1(9)$	$C_1(0)$	$C_1(1)$
	3	

TABLE IV: Third feature table of Color Pass

	$C_1(3)$	
$C_1(4)$	$C_1(5)$	$C_1(6)$
$C_1(7)$	$C_1(8)$	$C_1(9)$
$C_1(0)$	$C_1(1)$	$C_1(2)$
	4	

TABLE V: Fourth feature table Of Color Pass

	$C_1(4)$	
$C_1(5)$	$C_1(6)$	$C_1(7)$
$C_1(8)$	$C_1(9)$	$C_1(0)$
$C_1(1)$	$C_1(2)$	$C_1(3)$
	5	

TABLE VI: Fifth feature table of Color Pass

	$C_1(5)$	
$C_1(6)$	$C_1(7)$	$C_1(8)$
$C_1(9)$	$C_1(0)$	$C_1(1)$
$C_1(2)$	$C_1(3)$	$C_1(4)$
	6	

TABLE VII: Sixth feature table Of Color Pass

	$C_1(6)$	
$C_1(7)$	$C_1(8)$	$C_1(9)$
$C_1(0)$	$C_1(1)$	$C_1(2)$
$C_1(3)$	$C_1(4)$	$C_1(5)$
	7	

TABLE VIII: Seventh feature table of Color Pass

	$C_1(7)$	
$C_1(8)$	$C_1(9)$	$C_1(0)$
$C_1(1)$	$C_1(2)$	$C_1(3)$
$C_1(4)$	$C_1(5)$	$C_1(6)$
	8	

TABLE IX: Eighth feature table Of Color Pass

E. PIN Entry Mechanism in Color Pass

In this scheme, the user chosen PIN is four colors. During the login procedure, when the Feature Tables appear in the screen then the system throws some challenge values

	$C_1(8)$	
$C_1(9)$	$C_1(0)$	$C_1(1)$
$C_1(2)$	$C_1(3)$	$C_1(4)$
$C_1(5)$	$C_1(6)$	$C_1(7)$
	9	

TABLE X: Ninth feature table of Color Pass

	$C_1(9)$	
$C_1(0)$	$C_1(1)$	$C_1(2)$
$C_1(3)$	$C_1(4)$	$C_1(5)$
$C_1(6)$	$C_1(7)$	$C_1(8)$
	10	

TABLE XI: Tenth feature table Of Color Pass

to the user. The challenge is passed via a secured media and so only the user can access it. In our scheme, the user can receive the challenge via any interface method.

Challenge values range from 1 to 10. Based on the challenge value the user has to select the corresponding Feature Table. For example, challenge value 4 indicates that the user has to look in the Fourth Feature Table. The challenge values will be generated using pseudo-random function [21]. User will receive challenge corresponding to each color of his PIN. After listening to each challenge value, user selects a Feature Table. Then corresponding to the chosen color PIN, he locates the color cell in that table. The user then finds the digit in that color cell and enters that digit as response to the challenge. Similarly user will respond to the other three challenge values and will complete the login process. Valid response to the challenge values will authenticate the user. Methodology of evaluating user successfully response is given below.

Each color has been assigned a number from 0 to 9 by

Color Index	*Assigned Values*	*Assigned Colors*
C_0	0	*Yellow*
C_1	1	*Pink*
C_2	2	*White*
C_3	3	*Violate*
C_4	4	*Dark Green*
C_5	5	*Orange*
C_6	6	*Sky*
C_7	7	*Grey*
C_8	8	*Peach Puff*
C_9	9	*Green Yellow*

TABLE XII: Used colors for implementing feature tables

the system as shown in TABLE XIV. If user chooses four colors (say) C2C3C4C1, the system database stores user PIN as 2341. We have stored this user PIN in an array UCOL (indexed from 0 to 3). The four random numbers (challenge values) generated by system has been stored in array RAN (indexed from 0 to 3).User response to the challenge has been stored in array CLICK (indexed from 0 to 3). Array EVAL (indexed from 0 to 3) has been initialized by 0 initially. All these arrays have been used for implementing Algorithm 2. Algorithm 2-Evaluating User Response in Color Pass

Input: This algorithm will take array UCOL, array CLICK and array RAN as input.

DOI: 10.18535/ijecs/v5i6.10

Output: This algorithm will update value of array EVAL by
1 for each valid response. for i = 0 to 3 do
K RAN[i] 1
Valid (UCOL[i] + K) mod 10 if CLICK[i] := Valid then EVAL[i]
1 end if end for
In the above algorithm Valid holds the correct response value for each challenge.

F. Algorithm 3-User Authentication

Input: This algorithm will take array EVAL as input after executing Algorithm 2.
Output: Decides whether user is allowed to Login. Initialize
X := 0 for i = 0 to 3 do if EVAL[i] := 1 then
X 1 else X 0
break

User Chosen Color	Challenge	Response
C_2	5	6
C_3	7	9
C_4	2	5
C_1	5	5

TABLE XIII: User Response table for a given challenge

end if end for if X := 1
then Allow user to Login
else
Disallow the user end if
Suppose user has chosen PIN C2C3C4C1 and he gets the challenge values 5, 7, 2, 5. So first user will go to the 5th Feature Table (see TABLE VI) and enter the digit written on color C2 (i.e. 6). For the second challenge value 7 user will go to the 7th table (see TABLE VIII) and will enter the digit written on color C3 (i.e. 9). Valid response for each of the challenge values has shown in TABLE XIII.

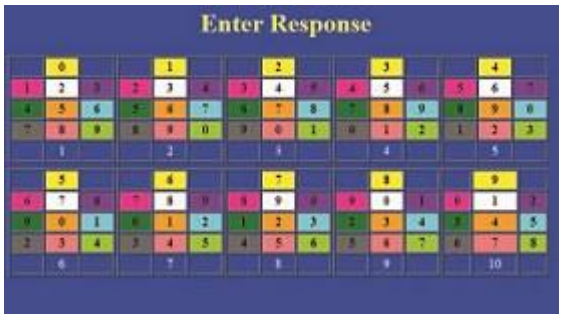


Fig. 3. Interface on Screen

Fig. 4. Interface for Entering Response

G. Mathematical Model

Mathematically, we can achieve the following: we ask a user to enter PIN of length n, the minimum length of username and Password is 4 number, then user will get the 4 number of challenge value by system.

Each Numeric value assign the unique color in registration phase. i.e. 0.9.There is implementation stages one by one as follows.

1) Implementation 1:- : Enter the User PIN of n Number from set A.
Set A-0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Set B-C0, C1, C2, C3, C4, C5, C6, C7, C8, C9
For example-PIN is 2341 then Color is from set C2, C3, C4, C1 then user will get the challenge value 5, 7, 2, 1.

2) Implementation 2:- : Create the Feature table by Mathematical formulation. Feature table of set F-F1,F2,F3,F4,F5,F6,F7,F8,F9,F10 and Cell Color Index of set B, for i=09 and j=09.
F(i).Cell(j).Color=Color(j) for the Color value and F(i).Cell(j).Value=(i+j)mod10 for the value of Cell.

3) Implementation 3:- : Enter the Response to system by Feature table with Challenge Values. Choose the PIN from set A and store the challenge values in one array as RAN[i=0,1,2,3] and Response from Click set C-i=0,1,2,3 then i= 0 to 3, K-General Store Function. K=RAN[i]-1 so then use Valid (A[i] + K) mod 10 if CLICK[i] := Valid

IV. RESULT ANALYSIS

The security and the usability of the proposed system are examined in this section.

A. Security Analysis

As the scheme is partially observable so the attacker cannot see the challenge values received by the user. Only the responses by the user are visible to the attacker. Thus to ensure security, the attacker should not able to guess the PIN just by seeing the responses. Suppose user has chosen color C5 as one of his secrete PIN and he gets a challenge 4

corresponding to that PIN digit. So a valid response from user will be 8 as per the Feature Tables described earlier. Now as attacker does not know the challenge value 4 and as digit 8 is printed upon all ten colors of all ten tables so attacker will not be able to retrieve the original color chosen by user. This makes Color Pass robust against shoulder surfing attack.

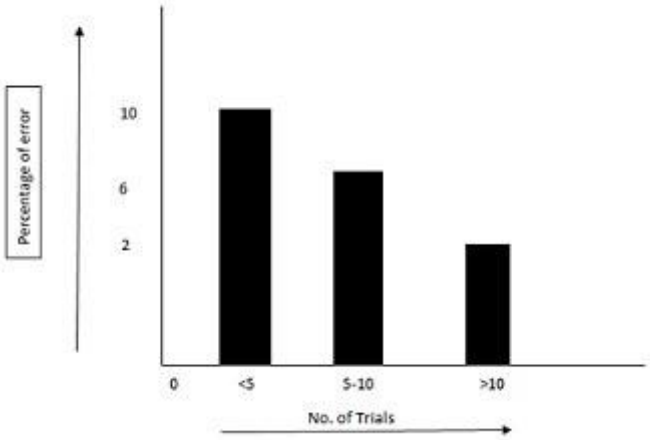
In terms of guessing attack, it has equal strength compared to a 4 digit PIN scheme. The probability of guessing during a session is 1/104 as for each color there are ten possibilities. The co-relation between user chosen colors cannot be guessed by an attacker which is an obvious advantage of Color Pass over SSSL.

Side channel attack [22] is another possible attack where human users are involved. Some variation of this attack is found in [23]. In this attack, the attacker tries to guess from the time the user takes to execute a particular operation. If the attacker can record the users reaction time, then SSSL is sensitive for such an attack. In the proposed Color Pass scheme, the user response time is expected to improve with each session as the orientation of the Feature Tables are fixed. So with each session user gradually gets familiar with the system and thus response time also improves. This makes side channel attack quite challenging for the Color Pass scheme.

B. Usability Evaluation

System implemented for use in public domain requires user friendliness along with mechanism to protect sensitive details of the users. In our proposed methodology, we have found it efficient against attack like Shoulder Surfing or guessing the password. Our evaluation of usability and feedback from users also appears satisfactory. We have performed our experiment using the following work station with configuration 4 GB RAM, i3 core processor and processing speed of 2.40 GHz. We took help of 20 users to perform our experiment. First we give a broad overview about how the methodology works. The average time taken by users to understand our methodology is about 10 minutes (mins). And the feedback we got from most of the users is that our methodology is very easy to understand. It should be noted that we only give the users lesson about how to use the system. Our lesson does not include security analysis of our proposed scheme. Each lesson period is about 5 mins. We chose the users from the students (12 students) and other persons from the society (8 people).

Compatibility of Color Pass in terms of use. After a discussion with users we give users about 30 mins to choose their password and for memorizing it. Then we asked the users to login with their password. We have performed our experiment in three phases. In Phase 1, number of trials is five or less. In Phase 2, number of trials considered is between 5 to 10. Number of trials greater than 10 times is considered under Phase 3. The login time is the duration of time taken by user to listen to 4 challenge values and give response to the challenge values during a session. Login time obtained from our experiment is shown in Figure 5. The percentage of error during login time is significantly low (less than 6 percentage) as the users get habituated (after 5 10 trails) with the system. The error rate for our experiment is shown in Figure 6.



The average login time is marginally improved (12 secs)

Fig. 5. Evaluation of user response

in Color Pass compared to modulo 10 table method (12.5 secs). However, the percentage of error during login process is much less (only 2 percentage) in Color Pass compared to modulo 10 table method which was approximately 15 percentage.

No special mathematical knowledge is required to use our scheme. Thus the scheme can be easily used by any type of users which widens the scope of applicability of our scheme. However one problem associated with our scheme is that scheme cannot be used by color blind people. As the scheme is based on colors only. Except this limitation our methodology is quite powerful against attacks such as guessing PIN, shoulder surfing attack, side channel attack and yet provides a simple to use interface which consumes a very low login time.

Number of users	Lesson Periods
8	1
8	2
2	3
2	more than 3

TABLE XIV: Time taken during learning

Number of users	Feedback
16	Easy to understand
3	Fairly Understandable
1	Not complicated

TABLE XV: User Feedback

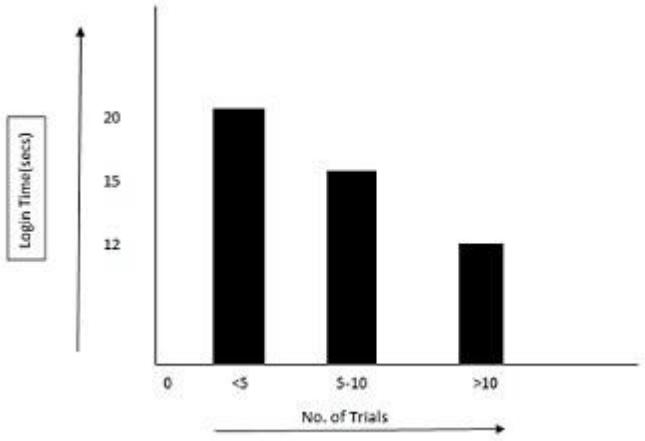


Fig. 6. Error during login

V. CONCLUSIONS

In this paper we have proposed a novel scheme to authenticate a user using color PINS. The scheme is known as Color Pass scheme which provides an intelligent interface for users to login into system in a public domain. In this scheme, the user remembers four colors as his PIN. The scheme works on the framework of partially observable attacker model. From security point of view the scheme is quite robust against some possible attacks such as shoulder surfing, guessing password, side channel attack, etc. And from usability point of view the scheme is user friendly and takes very less time for login. Also the scheme can be used by both math and non-math oriented people. The proposed methodology shows significant low error rate during login procedure. In future we will explore how to extend this scheme for fully observable attacker model.

REFERENCES

[1] S.Kumaresan, G.Dinesh Kumar, S.Radhika *Design of Secured ATM by Wireless Password Transfer and Shuffling Keypad* IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS15.

[2] C. Herley, P. C. Oorschot, and A. S. Patrick, *Passwords: If were so smart, why are we still using them?,* in Financial Cryptography, pp. 230237, 2009.

[3] *www.webeopdia.com/term/s/shouldersurfing.html* (last access October, 2013).

[4] L. Sobrado *Shoulder-surfing resistant graphical passwords,* Draft, 2005. (http://clam.rutgers.edu/ birget/grPssw/srgp.pdf)

[5] R. Dhamija, and A. Perrig. *Dj Vu: A User Study Using Images for Authentication.* In 9th USENIX Security Symposium, 2000.

[6] J.C. Birget *Shoulder-surfing resistant graphical passwords,*, 2005.

[7] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, *Design and evaluation of a shoulder-surfing resistant graphical password scheme,*

. Hartanto, B. Santoso, and S. Welly, *The usage of graphical password as a replacement to the alphanumerical password,* Informatika, vol. 7, no. 2, 2006, pp. 91-97.

. Man, D. Hong, and M. Mathews, *A shoulder surfing resistant graphical password scheme,* Proc. of the 2003 Int. Conf. on Security and Management, June 2003, pp. 105111 .

. Perkovic, M. Cagalj, and N. Rakic, *SSSL: shoulder surfing safe login,* Proc. of the 17th Int. Conf. on Software, Telecommunications Computer Networks, Sept. 2009, pp. 270-275.

. Zheng, X. Liu, L. Yin, and Z. Liu, *A stroke-based textual password authentication scheme,*Proc. of the First Int. Workshop. on Education Technology and Computer Science, Mar. 2009, pp. 90-95.

. Yamamoto, Y. Kojima, and M. Nishigaki, *A shouldersurfing-resistant image-based authentication system with temporal indirect image selection,* Proc. of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188194.

. Zhao and X. Li, *S3PAS: A scalable shoulder-surfing resistant textualgraphical password authentication scheme,* Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472.

[15] B. R. Cheng, W. C. Ku, and W. P. Chen, *An efficient loginrecording attack resistant graphical password scheme SectorLogin,* Proc. of 2010 Conf. on Innovative Applications of Information Security Technology,
Proc. of Working Conf. on Advanced Visual Interfaces, May. 2006, pp. 177-184.

[8] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, *Design and analysis of a graphical password scheme,* Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.
Dec. 2010, pp. 204-210.

[16] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. *Authentication schemes for session passwords using color and images,* International Journal of Network Security Its Applications, vol. 3, no. 3, May 2011.

[17] S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho. *A new shoulder-surfing resistant password for mobile environments,* Proc. of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 20 11.

[18] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, *A New Graphical Password Scheme Resistant to Shoulder-Surfin.*

[19] A. F. Syukri, 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.

[20] *searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last access october, 2013).*

[21] L. Blum, M. Blum, and M. Shub, *A simple unpredictable pseudorandom number generator,* SIAM Journal on Computing, vol. 15, pp. 364383, may 1986.

[22] P. C. Kocher, *Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems,* in CRYPTO, pp. 104113, 1996.

[23] L. Zhuang, F. Zhou, and J. D. Tygar, *Keyboard acoustic emanations revisited,* in ACM Conference on Computer and Communications Security, pp. 373382, 2005.