ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

Color Lock: Against Password Attacks

[1]Joelin Mary Jose, [2]Jannet Paul, [3]Pradeep P Mathew

[1,2] BTech,[3]Assistant Professor, MBCCET, Peermade, Idukki

Abstract: **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. Color password is widely famous, but it is prone to shoulder surfing attacks, in which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN. Traditional PIN-entry methods are vulnerable to a wide class of observation attacks such as brute force attacks, side channel attacks etc. A number of alternative PIN-entry methods that are based on human cognitive skills have been proposed till date. These methods can be classified into two classes regarding information available to a passive adversary: fully observable and partially observable. In this paper, we propose an intelligent user interface, known as Color Lock to resist the password attacks so that any genuine user can enter the session PIN without disclosing the actual PIN. The Color Lock is based on a partially observable attacker model. The experimental analysis shows that the Color Lock interface is safe and easy to use.**

Keywords: **Color PIN, Shoulder Surfing Attack, User Interface, Partially Observable.**

1. INTRODUCTION

There are a huge internet users in the world today. In a recent report [1], the number of Internet users has been reported as approximately 2.4 billion world wide, and from 2000 to 2012, it is a staggering 566.4% increase. These users can be both genuine and malicious users as well. Nowadays it is very important to know which user is genuine or malicious. Our proposed software applications deal with sensitive as well as private information which must be saved from misuse by some malicious or unauthorized users and their attacks. Every security area, role of authentication is a very important technique by which the system can identify the type of users. There are many authentication schemes available among which password based authentication is most used as it is cost effective and secure. The shoulder surfing attack in an attack that can be performed by the opponent to obtain the user's password by watching over the user's shoulder as he enters his password .The classical PIN entry mechanism is widely used because of its ease of usability and security, but it often leads to shoulder surfing attack in which a user can record the login session and retrieve the user original PIN for misuse in future.

Based on the information available to the attacker, secure login methods can be classified into two broad categories completely observable and partially observable. In the first one, the attacker can completely observe the whole login procedure for a particular session and use it to gain knowledge about the actual pin and in the second one, the attacker can partially watch the login procedure. Our proposed system is partially observable and users have to remember four color pins. In the proposed methodology, we use session pin without disclosing actual pin.

In the proposed system, the user sets four color as their pin. User has to answer four challenge question corresponding to each color. Here, the user has to remember four color instead of remembering long alpha-numeric passwords. It is difficult for the users to remember long alpha-numeric passwords or graphical passwords and also they are prone to brute force and shoulder surfing attacks. At the same time, Color Lock provides equal password strength compared to conventional pin entry mechanisms.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

2. EXISTING SYSTEM

2.1 Mod 10 method:

In this work G.T Wilfong [2] proposed a methodology where user has to perform a simple mathematical operation. User has to remember a four digit PIN number from the set {0, 1,..., 9}. User receives a challenge from the set {0, 1,..., 9} via a protected media. User will add the challenge digit with the corresponding PIN digit and will perform a modulo 10 operation. Then we will enter back the number obtained. Suppose the first digit of the user chosen PIN is 5. User now securely receives a challenge 7 from the system. So the valid response by user will be (5+7) modulo 10 (which is equal to 2). Though this method is easy to execute and gives good security and is also easy for math-oriented people. But for non-math-oriented people this methodology is difficult to adopt. So other methods were developed to enhance this method.

2.2 Shoulder surfing safe login:

Unlike the previous two schemes, in SSSL, proposed by Perkovic et al. [3], user does not provide any number as response rather enters some direction to the system.

This method Shoulder Surfing Safe Login (SSSL) involves a protected channel through which a user receives challenges. SSSL does not require users to perform any complicated mathematical or mentally demanding operation. The design choice to include the protected channel in scheme (SSSL) was motivated by the following observations. Firstly, designing secure cognitive PIN-entry schemes in the "fully observable" model is challenging as the SAT solver attack show. Secondly, secure PIN-entry schemes from this model involve multiple rounds of a basic challenge response protocol and they require users to perform complicated mathematical calculations, which is a major deterrent to the acceptance of such technology (an average time of about 166 seconds).

The SSSL PIN-entry scheme implements the one-time pad paradigm. Thus, to enter a single digit of a secret PIN, a user first receives a challenge (a random number between 1 and 9) from an interrogator (computer, ATM) over a channel that ensures secrecy and integrity (e.g., via earphones). Next, the user visually locates the received challenge in a special table of digits displayed on his/her computer's screen. Finally, theuser responds by clicking on the appropriate button (shown on the computer's screen) that uniquely links the secret challenge with the secret digit of the PIN.

SSSL does not require any numerical computation on the part of the human user. Moreover, the number of challenge-response rounds equals the size of the PIN. It is these two features that make the SSSL easy to use and very user friendly.

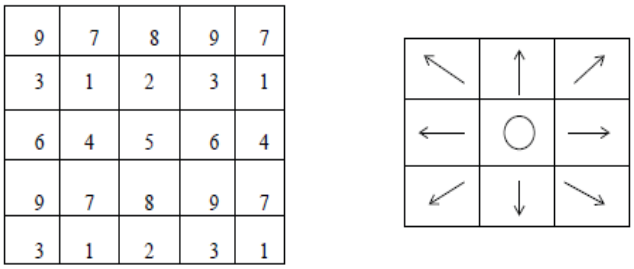

Fig 1: (a) orientation of digits (b)keypad structure

3. PROPOSED METHODOLOGY

The proposed methodology, ColorLock provides an interface which is partially observable. The attacker can only see the response given back to the system but cannot see the challenge questions generated by the system. Thus it is assumed that the media through which user gets the challenge should ensure security against man-in-middle attack [4].

3.1 Characteristics of user pin:

In our scheme the color is used to form a PIN instead of remembering conventional passwords. User can choose four colors from a set of ten different colors represented as {C0, C2,•••,C9}. User can choose one color more than once. So one possible instance of user chosen PIN might be C1C2C1C4. Each Ci denotes a specific color (say blue or white). As user chosen PIN is comprised of four colors so probability of guessing the PIN will be 1/104.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

3.2Login procedure:

Here, we will discuss about how the user interacts with the system:

• User enters his login id.

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

• 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 using Algorithm 2.

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

The user connects to a system by following the above steps[5]

3.3 Characteristics of feature table:

Color Lock 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 position 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.

Table 1: Identifying Each Cells in kth table

	0	
1	2	3
4	5	6
7	8	9
	k	

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,V i > 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. All the ten Feature Tables are shown in Table 2 to Table 9. The numbers written in bold denotes the table number of each Feature Table. The empty cells in the tables denote nothing.

3.4 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 let's 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 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 LOCK:

```
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
```

Thus using Algorithm 1, all the cells of ten Feature Tables

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

Table 2:First feature table of Color Pass

	$C_0(0)$	
$C_1(1)$	$C_2(2)$	$C_3(3)$
$C_4(4)$	$C_5(5)$	$C_6(6)$
$C_7(7)$	$C_8(8)$	$C_9(9)$
	1	

Table 3: Second feature table of Color Pass

	$C_0(1)$	
$C_1(2)$	$C_2(3)$	$C_3(4)$
$C_4(5)$	$C_5(6)$	$C_6(7)$
$C_7(8)$	$C_8(9)$	$C_9(0)$
	2	

Table 4: Third feature table of Color Pass

	$C_0(2)$	
$C_1(3)$	$C_2(4)$	$C_3(5)$
$C_4(6)$	$C_5(7)$	$C_6(8)$
$C_7(9)$	$C_8(0)$	$C_9(1)$
	3	

Table 5: Fourth feature table of Color Pass

	$C_0(3)$	
$C_1(4)$	$C_2(5)$	$C_3(6)$
$C_4(7)$	$C_5(8)$	$C_6(9)$
$C_7(0)$	$C_8(1)$	$C_9(2)$
	4	

Table 6: Fifth feature table of Color Pass

	$C_0(4)$	
$C_1(5)$	$C_2(6)$	$C_3(7)$
$C_4(8)$	$C_5(9)$	$C_6(0)$
$C_7(1)$	$C_8(2)$	$C_9(3)$
	5	

Table 7: Sixth feature table of Color Pass

	$C_0(5)$	
$C_1(6)$	$C_2(7)$	$C_3(8)$
$C_4(9)$	$C_5(0)$	$C_6(1)$
$C_7(2)$	$C_8(3)$	$C_9(4)$
	6	

Table 8: seventh feature table of Color Pass

	$C_0(6)$	
$C_1(7)$	$C_2(8)$	$C_3(9)$
$C_4(0)$	$C_5(1)$	$C_6(2)$
$C_7(3)$	$C_8(4)$	$C_9(5)$
	7	

Table 9:Eight feature table of Color Pass

	$C_0(7)$	
$C_1(8)$	$C_2(9)$	$C_3(0)$
$C_4(1)$	$C_5(2)$	$C_6(3)$
$C_7(4)$	$C_8(5)$	$C_9(6)$
	8	

Table 10:Ninth feature table of Color Pass

	$C_0(8)$	
$C_1(9)$	$C_2(0)$	$C_3(1)$
$C_4(2)$	$C_5(3)$	$C_6(4)$
$C_7(5)$	$C_8(6)$	$C_9(7)$
	9	

Table 11:Tenth feature table of Color Pass

	$C_0(9)$	
$C_1(0)$	$C_2(1)$	$C_3(2)$
$C_4(3)$	$C_5(4)$	$C_6(5)$
$C_7(6)$	$C_8(7)$	$C_9(8)$
	10	

3.5 PIN Entry Mechanism in Color Lock:

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 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 a headphone.

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 psudo-random function [6]. User will receive challenge corresponding to each color of his PIN.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

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.

Table 12 : Used colors for implementing feature tables

Color Index	*Assigned Values*	*Assigned Colors*
C_0	0	*Yellow*
C_1	1	*Pink*
C_2	2	*White*
C_3	3	*Violaue*
C_4	4	*DarkGreen*
C_5	5	*Orange*
C_6	6	*Sky*
C_7	7	*Grey*
C_8	8	*PeachPuff*
C_9	9	*GreenYellow*

Each color has been assigned a number from 0 to 9 by the system as shown in Table 12 . 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.

ALGORITH 2: EVALUATING USER RESPONSE IN COLOR LOCK

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

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
  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

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

Table 13 : User Response table for a given challenge

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

Feature Table and enter the digit written on color C2 (i.e. 6). For the second challenge value 7 user will go to the 7th table and will enter the digit written on color C3 (i.e. 9). Valid response for each of the challenge values has shown in Table 13.

4. USER INTERFACE FOR COLOR LOCK

While implementing user interface we have assigned unique colors to each Ci (i varies from 0 to 9) (shown in TABLE XIV). Ten colors is chosen in such a way so that each color is clearly distinguishable from other. The actual interface is shown in Fig. 2. For convenience we have marked each table number by white font to distinguish it from other digits (which are marked using black font) in the table. As the color cell's position in each table is fixed so user can locate the desired colored cell quite quickly. This contributes in getting faster login time. The tables are designed in such a way so that the user interface does not look too clumsy and also the screen space is used in an optimum manner.

Similarities between keypads in Color Lock, as shown in Fig. 3 and classical PIN entry method makes our methodology more user friendly. Only the two extreme keys at the bottom row are kept unused. If user chooses Yellow Pink Violate Grey and receives challenge values 6356then seeing the interface in Fig. 2 user will enter 5372using the key board showing at Fig. 3.

5. SECURITY AND EVALUATION STUDY OF COLOR PASS

Some of the salient features of the proposed Color Pass scheme is described in the followings. Mainly two broad aspects - security and usability are discussed next.

5.1 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 Lock 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 color cannot be guessed by an attacker which is an obvious advantage of Color Lock over SSSL.

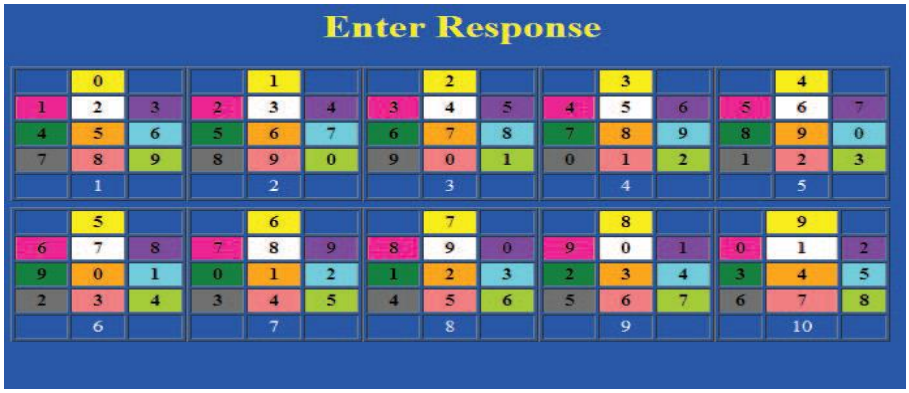

Fig. 2: User Interface On Screen

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (148-156), Month: April - June 2016, Available at: www.researchpublish.com

Fig. 3: User Interface for Entering Response

Side channel attack [7] is another possible attack where human users are involved. Some variation of this attack is found in [8]. 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 user's reaction time, then SSSL is sensitive for such an attack. In the proposed Color Lock 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 Lock scheme.

5.2 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).

Table14 : Time taken during learning

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

Table15 : User Feedback

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

Table 14 and Table 15 show an evaluation of compatibility of Color Lock in terms of use. After a discussion with users we give users about 30 mins to chose 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 4. The percentage of error during login time is significantly low (less than 6%) as the users get habituated after 5 − 10 trails) with the system. The error rate for our experiment is shown in Figure 5.The average login time is marginally improved (12 secs) in Color Lock compared to modulo 10 table method (12.5 secs). However, the percentage of error during login process is much less (only 2%) in Color Lock compared to modulo 10 table method which was approximately 15%.

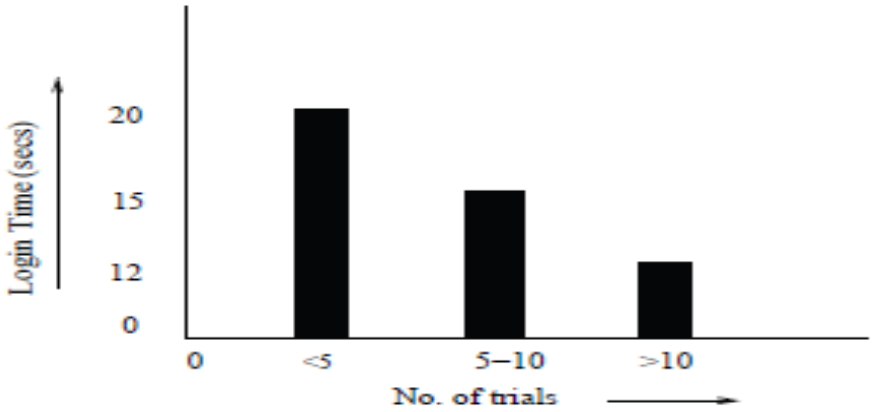

Fig. 4: Evaluation of user response

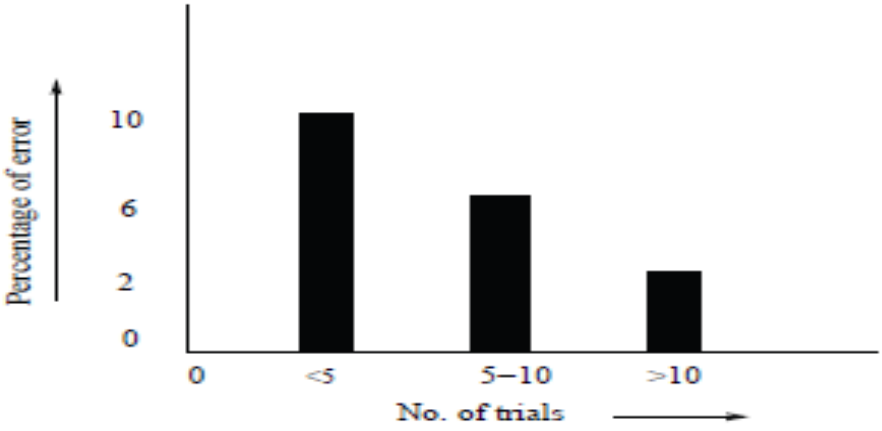

Fig. 5: Error during login

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.

6. CONCLUSION AND FUTURE WORK

In this paper we have proposed a novel scheme to authenticate a user using color PINS. The scheme is known as Color lock 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.

ACKNOWLEDGMENTS

This work is partially supported by a research grant from the Science and Engineering Research Board (SERB), Government of India, under sanction letter no. SB/FTP/ETA- 226/2012.

REFERENCES

[1] M.M. Group, "http://www.internetworldstats.com/stats.htm," June 2012.

[2] G. Wilfong, "Method and appartus for secure pin entry." US Patent No. 5,940,511, In Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1997.

[3] T. Perkovic, M. Cagali, and N. Rakic, "SSSL: Shoulder surfing safe login," in Software Telecommunications and Computer Networks, pp. 270–275, 2009.

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

[5] Colorpass: an intelligent user interface to resist shoulder surfing attacks.

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

[7] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1996.

[8] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in ACM Conference on Computer and Communications Security, pp.373–382, 2005.