The Modified Authentication Scheme to Defy Shoulder Surfing Attack

Latha. R
Department of Computer Science and Engineering
EBET Group of Institutions, Nathakadaiyur
Kangayam, India 638108

Ms.Kavitha. M.N, AP
Department of Computer Science and Engineering
EBET Group of Institutions, Nathakadaiyur
Kangayam, India 638108

***Abstract*— Personal Identification Number is a well-known authentication method used in Automated Teller Machine. Classical pin entry schemes are widely used because it provides fair security and easy to use. However, when used in public domain it is vulnerable to shoulder surfing attack.To avoid such attack, we have proposed a methodology known as an enhanced password authentication scheme to defy shoulder surfing attack using colors. In the proposed scheme, user remembers a password consisting of colors only and the responses are provided by some digits with the help of system generated challenge values and those values are sent to user's mobile. In the proposed scheme user does not disclose their actual pin. Experimental analysis shows that our scheme is less error prone, easy to use and provides high security compared to existing approaches.**

Keywords— Personal Identification Number, Color PIN, Shoulder Surfing Attack, User Interface, Password.

I. INTRODUCTION

The number of internet users is rising in recent years. These huge numbers of users consist of both genuine users and malicious users. So software applications that deal with sensitive information should provide a strong protection to the system so that authorized 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 commonly used for its ease of use and cost effectiveness.

Authentication is a process by which system verifies the identity of a user. Classical PIN entry mechanism is widely used for authenticating a user. However, when used in public domain it is prone to shoulder surfing attack. In this the attacker observes the entire login session and may guess the user's original pin. To avoid such attack, in this scheme colors are used to form the pin. Each time the pin varies so the attacker cannot able to find the pin by observing the login session. The Personal identification number (PIN) is a numeric password shared between the user and a system. It is used to authenticate the user to the system. The user is granted access only if the pin matches. The proposed methodology implements one time pass paradigm. Thus corresponding to four color PINs, the user gets four challenges and enters his response with respect to each challenge value.

The main objective of Color scheme is that it is easy to use and it does not require any special knowledge. It provides equal password strength as compared with the conventional PIN entry scheme.

The rest of the paper is organized as follows- Section II is about some existing methodologies proposed for partially observable system. In Section III, the proposed Color Pass scheme has been discussed in detail. The user interface for Color Pass has been described in Section IV. Finally we conclude in Section V and give future direction of our work.

II. RELATED WORK

There are many graphical password techniques, used to resist shoulder surfing attack but it is expensive. Biometrics includes finger prints, iris scan or facial recognition. It is costly and difficult to implement. The identification process is slow. The following are some methods that motivated us to propose the color scheme.

A.Mod 10 method

In this G.T Wilfong [9] proposed a methodology where user has to perform a simple mathematical operation. User remembers 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. Finally he will enter back the obtained digit using a public keyboard. Suppose the first digit of the user chosen PIN is 4 and the challenge value from the system is 7 then the user response will be (4+7) modulo 10 which is equal to 1. This method is easy for math oriented people but difficult for non math oriented people.

B. Mod 10 table method

In this method Perkovic [10] proposed a concept of lookup table. If user chosen PIN digit is 6 and the system generated challenge is 9 then the user first goes to the row number 6 in the lookup table and subsequently goes to the digit 9 in that row. After that user will see the corresponding column number where 9 is placed (here 1) and enter back 1 as response corresponding to the first challenge.

	6	3	9	4	8	1	7	2	5	0
0	0	1	2	3	4	5	6	7	8	9
1	9	0	1	2	3	4	5	6	7	8
2	8	9	0	1	2	3	4	5	6	7
3	7	8	9	0	1	2	3	4	5	6
4	6	7	8	9	0	1	2	3	4	5
5	5	6	7	8	9	0	1	2	3	4
6	4	5	6	7	8	9	0	1	2	3
7	3	4	5	6	7	8	9	0	1	2
8	2	3	4	5	6	7	8	9	0	1
9	1	2	3	4	5	6	7	8	9	0

TABLE I: User Lookup Table

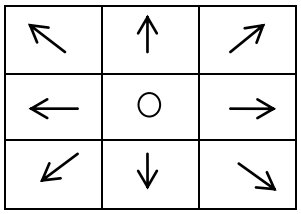
If the digits in the top row of Table I is arranged in ascending order from 0 to 9 then it will be equivalent as modulo 10 addition. Hence the name of the table is justified. But one of the drawback of this procedure is login time in this method goes high with respect to modulo 10 method. The error rate does not improve much with the number of attempts.

C. Shoulder Surfing Safe login

In SSSL, proposed by Perkovic [11], user does not provide any number as response rather enters some direction to the system.

9	7	8	9	7
3	1	2	3	1
6	4	5	6	4
9	7	8	9	7
3	1	2	3	1

(a)



(b)

Fig. 1: (a) Orientation of digits (b) Keypad structure for SSSL

In this scheme user remembers a five digits PIN. The user has to answer to the challenge values throws to him with respect to the table and keypad consist of arrows shown in Fig.1. The table in SSSL method is constructed in such a way that every digit i is an immediate neighbor to other 8 digits from the set {1, 2, ...9} (see Fig.1(a)). User locate the relative position of their original PIN digits and the challenge values via keypad shown in Fig.1(b). The following example will give a clear idea about SSSL methodology.

PIN	Challenge	Response
9	3	↑
6	6	○
9	5	↖
7	7	○
8	1	↙

TABLE II: User response table of SSSL

Suppose user chosen pin is 96978, and the corresponding challenge value is 36571. As digit 3 is placed under the value 9 in Fig.1 (a) so the user will press the down arrow. When the PIN digit is 6 and the challenge is also 6 then the response is press ◦ key. However, in SSSL the existence of co-relation between digits can be observed by a clever attacker and he may use it to guess the PIN.

III. PROPOSED METHODOLOGY

The proposed system use new authentication technique that consists of three phases: registration phase, login phase and verification phase. During the registration phase user choose four colors. In login phase user enters their username and password, if it is valid then the color interface will be displayed and four random numbers will be sent to the mobile. Based on the random number and the color, user will enter the pin. The system verifies the pin entered by comparing with the color choosed during registration.

A. Characteristic of user chosen PIN

In conventional PIN entry schemes it is required to remember either few digits as user PIN. But in our scheme the colors are used to form the PIN. User can choose four colors from the set of ten different colors represented as $\{C_0, C_1,\ldots C_9\}$. User has the flexibility to choose one color more than once. Each C_i denotes a specific color. As user chosen PIN is comprised of four colors so probability of guessing the PIN will be $1/10^4$.

B. 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 using Algorithm1.
- System then generates four random challenge values ranges from $1 \cdot \cdot \cdot 10$ and sent to user's mobile.
- Next user will have to give response to those challenge values.
- User response will be evaluated by system using Algorithm 2.
- Finally system will decide whether the user is legitimate or not using Algorithm 3.

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

C. Characteristic of Feature Tables

Color 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 C_i denotes the color of the cell i and V_i denotes the digit corresponding to cell i. C_i is unique with respect to a Feature Table. All cells in a table also contain a unique value V_i from the set {0,1,...,9}. Another important characteristic 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.

	0	
1	2	3
4	5	6
7	8	9
	k	

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

D. Algorithm for Generating Tables

Suppose ten different colors $\{C_0, C_2,...,C_9\}$ 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 F T (i) and each cell is represented by CELL(j). So to refer a cell of a table we use the operator F T (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

F T (7).CELL(4).Color

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

F T (7).CELL(4).V alue

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 F T (0) · · · F T (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 will be initialized with some unique color and digit combination. Each color is assigned an unique number.

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

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

TABLE IV: First feature table

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

TABLE V: Second feature table

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

TABLE VI: Third feature table

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

TABLE VII: Fourth feature table

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

TABLE VIII: Fifth feature table

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

TABLE IX: Sixth 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 X: Seventh feature table

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

TABLE XI: Eighth feature table

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

TABLE XII: Ninth feature table

TABLE XIII: Tenth feature table

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 to the user. The challenge value is passed via mobile.

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 [13]. User will receive challenge corresponding to each color of his PIN.

User selects the Feature Table based on the challenge value. 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. The following method is used to evaluate the user based on the response given by the user.

Color index	Assigned values	Assigned colors
C_0	0	Red
C_1	1	Blue
C_2	2	Green
C_3	3	Yellow
C_4	4	Maroon
C_5	5	Grey
C_6	6	Pink
C_7	7	Purple
C_8	8	Brown
C_9	9	Aqua

TABLE XIV: Used colors for implementing feature tables

Each color has been assigned a number from 0 to 9. If user chosen colors are $C_2C_3C_4C_1$, 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 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.
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 $C_2C_3C_4C_1$ and he gets the challenge values 5, 7, 2, 5. So first user will go to the 5th

user chosen color	challenge	response
C_2	5	6
C_3	7	9
C_4	2	5
C_1	5	5

TABLE XV: User Response table for a given challenge

Feature Table (see TABLE VIII) and enter the digit written on color C_2 (i.e. 6). Valid response for each of the challenge values has shown in TABLE XV.

IV.USER INTERFACE FOR COLOR PASS

While implementing user interface we have assigned unique colors to each C_i (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. 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.

If user chooses Yellow Pink Purple Grey and receives challenge values 6 3 5 6 then seeing the interface in which user will enter 7 9 5 2 using the key board showing at Fig. 3.

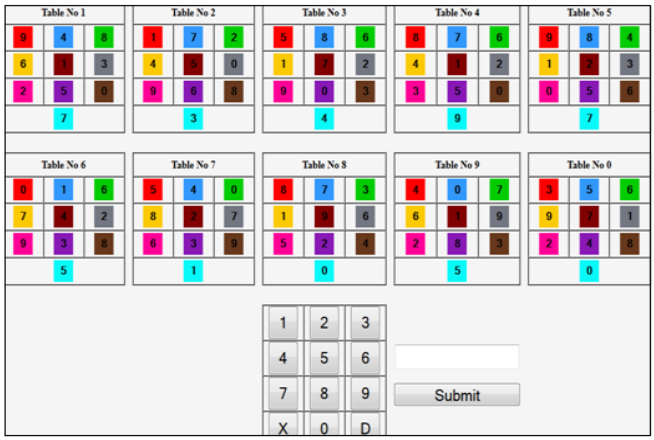


Fig 3. User interface and response

V. CONCLUSION

This scheme is used to authenticate the user using color pins. In this user remembers four colors as their pin. The user does not enclose his actual pin. The colors are used to form their pin. No special mathematical knowledge is required to use this. Thus the scheme can be easily used by any type of users which widens the scope of applicability. 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.

REFERENCES

[1]M.M.Group,"http://www.internetworldstats.com/stats.htm," June2012.
[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. 230–237, 2009.
[3]"www.webeopdia.com/term/s/shoulder−surfing.html (last access October, 2013)."
[4] A. Paivio, "Mind and its evaluation: A dual coding theoretical approach," 2006.
[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] 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. 1-2, pp. 102–127, 2005.
[7] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in21st International Conference on Advanced Information Networking and Applications Workshops, pp. 467–472, 2007.
[8] G. E. Blonder, "Graphical passwords. in lucent technologies, inc., murray hill, nj, u. s. patent, united states," June 1996.
[9] 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.
[10] T.Perkovic,M.˝Cagalj, and N.Saxena, "Shouldr-surfing safe login in a partially observable attacker model," inSion, R.(eds.) FC 2010. LNCS, pp. 351–358, 2010.
[11] T. Perkovic, M. Cagali, and N. Rakic, "SSSL: Shoulder surfing safe login," inSoftware Telecommunications and Computer Networks, pp. 270–275, 2009.
[12] "Searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last access October, 2013)."
[13] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM Journal on Computing, vol. 15, pp. 364–383, may 1986.
[14] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1996.
[15] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in ACM Conference on Computer and Communications Security, pp. 373–382, 2005.