



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

A Survey On Avoid Shoulder Surfing Attack Using MultiColor Password

Priyanka R. Wajage¹, Priyanka D. Borhade², Priyanka S. Dahitule³

B.E. Students, Dept. of Computer Engineering, Jaihind College of Engineering, Pune, India

ABSTRACT: There are a large number of Internet users around the world. Our software applications deal with sensitive as well as private information which must be saved from misuse by some malicious users and their attacks. Hence 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 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 user the login methods can be categorized into fully observable and partially observable. In fully observable attack the user can fully observe the entire login procedure and in partially observable attack the user can partially observe the login session. The existing Color Pass methodology provides onetime pass paradigm corresponding to four color PINs in which the user gets four challenges for which the user enter response to each challenge. Its easy to use and doesnt require any additional knowledge. This method leads to drawback as the user uses the headphones to get the color values. Sometimes the headphones will not work properly or the user does not have the clarity in hearing, this leads to the poor understanding of the challenge values. Here 0-9 Feature tables are generated which increases the user response time. To overcome the disadvantage in the proposed method Multi Color Pass system the color values will be received via mobile phone. Instead of Feature Table we generate lookup table randomly.

KEYWORDS: Shoulder Surfing Attack, Color Pass, Classical PIN, Partially Observe, Lookup Table.

I. INTRODUCTION

The shoulder surfing attack is an attack that can be processed by the opponent to obtain the user's password by watching over the user's shoulder as he enters his password .As now a day there are a large Internet users in the world. Our proposed software applications deal with sensitive as well as private information which must be saved from misuse by some unauthorized users and their attacks. Every security process, authorization is a very important by which the system can guessing 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.

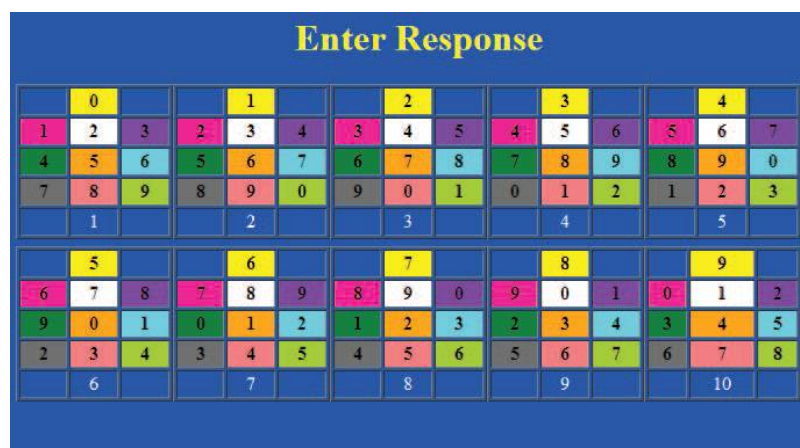
Based on the information available to the user the login methods can be categorized into fully observable and partially observable. In fully observable attack the user can fully observe the entire login procedure and in partially observable attack the user can partially observe the login session. The existing Color Pass methodology provides onetime pass paradigm corresponding to four color PINs in which the user gets four challenges for which the user enter response to each challenge. It's easy to use and doesn't require any additional knowledge. This method leads to drawback as the user uses the headphones to get the color values. Sometimes the headphones will not work properly or the user does not have the clarity in hearing, this leads to the poor understanding of the challenge values.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Here 0-9 Feature tables are generated which increases the user response time. To overcome the disadvantage in the proposed method Multi Color Pass system the color values will be received via mobile phone. Without generating Feature Table we generate lookup table randomly .In this system it also provides equal number of password strength as classical PIN entry .Refer Fig 1.as given below.



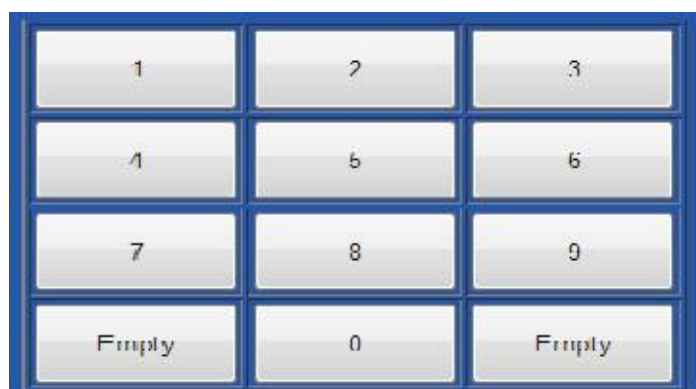
The figure shows a grid titled "Enter Response" with 10 columns and 5 rows. Each column is headed with a number from 0 to 9. The cells contain numbers from 0 to 9, with some cells being empty. The numbers are color-coded: yellow for the header, pink for the first row, orange for the second row, green for the third row, red for the fourth row, and blue for the fifth row.

	0		1		2		3		4					
1	2	3	2	3	4	3	4	5	4	5	6	5	6	7
4	5	6	5	6	7	6	7	8	7	8	9	8	9	0
7	8	9	8	9	0	9	0	1	0	1	2	1	2	3
	1		2		3		4		5					
	5		6		7		8		9					
6	7	8	7	8	9	8	9	0	9	0	1	0	1	2
9	0	1	0	1	2	1	2	3	2	3	4	3	4	5
2	3	4	3	4	5	4	5	6	5	6	7	6	7	8
	6		7		8		9		10					

Fig 1 .Generate Feature Table

II. RELATED WORK

To login the system, user first enter his own login-id and the user has to enter password in a correct manner, pass the four determined number of challenges. Our system is based on partially observable schemes which have motivated us to propose the Color Pass scheme for avoiding shoulder surfing attack. Consider the Fig 2 of Resposne Table for entering the response and get login to the system for transactions.



The figure shows a 4x3 grid of buttons. The buttons contain the numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, and two empty cells.

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

Fig 2 .Response Table

III. PROPOSED ALGORITHM

A. Design Considerations:

- 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 $\langle C_i, V_i \rangle$.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

- Here C_i denotes the color of the cell i and V_i indicates the digit corresponding to cell i .
- C_i 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 1 and this is fixed for every table.
- So if first cell of a table is filled with C_1 then first cell of all other tables are also filled with C_1 .

	0	
1	2	3
4	5	6
7	8	9
	k	

Table 1. Identifying Each Cells in k^{th} table

- All cells in a table also contain a unique value V_i from the set $\{0, 1, \dots, 9\}$. Another important characteristic is that in each cell i , the pair $\langle C_i, V_i \rangle$ is unique with respect to all the cells in all the ten tables.

B. Description of the Proposed Algorithm:

Suppose ten different colors $\{C_0, C_2, \dots, C_9\}$ 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 $FT(i)$ 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 :

$FT(7).CELL(4).Value$

IV. PSEUDO CODE

Algorithm 1: Generating tables in Color Pass

Step 1: This algorithm will take array `Color [0,1,...,9]` as input.

Step 1: It will generate Feature Tables $FT(0) \dots FT(9)$

for $i = 0$ to 9 do

for $j = 0$ to 9 do

$FT(i).CELL(j).Color \leftarrow Color[j]$

$FT(i).CELL(j).Value \leftarrow (i+j) \bmod 10;$

end for

end for

Algorithm 2 : Evaluating User Response in Color Pass

Step 1: This algorithm will take array `UCOL`, array `CLICK` and array `RAN` as input.

Step 2: This algorithm will update value of array `EVAL` by 1 for each valid response.

for $i = 0$ to 3 do

$K \leftarrow RAN[i] - 1$

$Valid \leftarrow (UCOL[j] + K) \bmod 10$

if $CLICK[i] := Valid$ then

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

```
EVAL[i] ← 1  
end if  
end for
```

Algorithm 3: User Authentication

Step 1: This algorithm will take array EVAL as input after executing Algorithm 2.

Step 2: 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
```

V. SIMULATION RESULTS

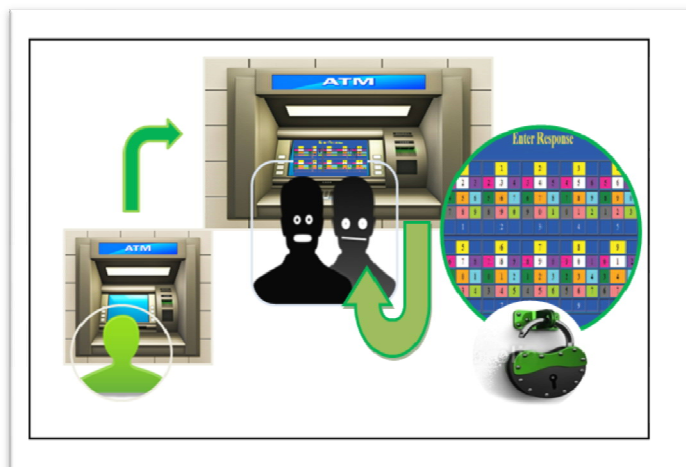


Fig 4.Result Screen

- 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.



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

VI. 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 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. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, vol. 2. Canada, 2007, pp. 467-472.
2. Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" *Journal of Computers*, vol.5, no.5 May 2010.
3. L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," *SIAM Journal on Computing*, vol. 15, pp. 364–383, may 1996.
4. 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.
5. L. Sobrado and J. C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002
6. B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumeric password," *Informatika*, vol. 7, no. 2, 2006, pp. 91-97.
7. 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.

BIOGRAPHY

Priyanka Wajage, Priyanka Dahitule and Priyanka Borhade are BE Students in the Computer Engineering Department, Jaihind College of Engineering(Pune), Savitribai Phule, Pune.