An Innovative Approach to Resist Shoulder Surfing Attack using Color Pass

Ameya Thakare[1] Piyush Deolasi[2] Sagar Ladwanshi[3] Deepak Makre[4]
[1,2,3,4]K K Wagh Institute of Engineering Education and Research, Nashik

Abstract— Classical PIN entry mechanism is widely used for authenticating a user. It is used on different platforms. But, this scheme suffers to shoulder surfing attack if used in public systems. In this attack, an unauthorized user can fully or partially observe the login session. The steps of the login session can be recorded or saved which the attacker can use it later to get the original PIN. In this project, we propose an intelligent user interface, 'Color Pass' to resist the shoulder surfing attack so that any authorized user can enter the login session's PIN without disclosing the original PIN. The purposed methodology is based on a partially observable attacker model. The analysis shows that the Color Pass interface is safe and easy to use even for users. This method is suitable for Personal Digital Assistants, Mobile phones, ATM pin entry mechanism, Laptops and Desktops.

Key words: Color PIN, Shoulder Surfing Attack, User Interface, Password, Partially Observable

I. INTRODUCTION

In a recent report, the number of Internet users has been reported as approximately 2.4 billion worldwide, and from 2000 to 2012, it is 566.4% increase. This user consists of both authorized users and unauthorized users. So applications which deal with private information must provide a sound based protection to login system so that authorized and unauthorized users can be recognized properly. In computer security, authentication is a technique by which the system identifies the authorized users. Among different authentication techniques, password based authentication is widely accepted solution for its ease use and cost effectiveness. Conventional PIN entry mechanism is widely famous for ease use and cost effectiveness, but still it is prone to shoulder surfing attack in which an attacker record's the login activity of a user for an entire login session and access the user actual PIN. Based on the information available to the attacker, secure login methods can be distributed into two 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 session. Our color pass 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. In addition to the resistance against shoulder surfing attack, it provides equal password strength as compared with the conventional PIN entry technique.

II. ALGORITHM

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

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

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

III. SOLUTION

In the paper "Color Pass: An intelligent user interface for resisting shoulder surfing attack" by N. Chakraborty and S. Mondal gave the solution to resist shoulder surfing attack. The proposed Color Pass interface is 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. In below section we first discuss about the characteristic of user chosen PIN. Then we have discussed user login procedure for a session. Then we give details about the structure and characteristics of tables used in implementing Color Pass. And at last there are details about PIN entry mechanism using our color pass method.

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 {C_0, C_2, ..., C_9}. User has the flexibility to choose one color more

than once. So one possible instance of user chosen PIN might be $C_1C_2C_1C_4$. Each C_i 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 $1/10^4$.

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 using Algorithm for generating 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 using Algorithm generating user response.
- Finally system will decide whether the user is legitimate or not using Algorithm for user authentication.

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 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 coloroccupies 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 iffirst 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 kth table

All cells in a table also contain a unique value V_i 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 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 $\{C_0, C_2,...,C_9\}$ 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 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 5^{th} 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

Thus using Algorithm for generating feature tables, all the cells of ten Feature tables will be initialized with some unique color and digit combination.

	C0(0)	
C1(1)	C2(2)	C3(3)
C4(4)	C5(5)	C6(6)
C7(7)	C8(8)	C9(9)
	1	

Table 2: First Feature table

	C0(1)	
C1(2)	C2(3)	C3(4)
C4(5)	C5(6)	C6(7)
C7(8)	C8(9)	C9(0)
	2	

Table 3: Second Feature table

	C0(2)	
C1(3)	C2(4)	C3(5)
C4(6)	C5(7)	C6(8)
C7(9)	C8(0)	C9(1)
	3	

Table 4: Third Feature table

	C0(3)	
C1(4)	C2(5)	C3(6)
C4(7)	C5(8)	C6(9)
C7(0)	C8(1)	C9(2)
	4	

Table 5: Fourth Feature table

	C0(4)	
C1(5)	C2(6)	C3(7)
C4(8)	C5(9)	C6(0)
C7(1)	C8(2)	C9(3)
	5	

Table 6: Fifth Feature table

	C0(5)	
C1(6)	C2(7)	C3(8)
C4(9)	C5(0)	C6(1)
C7(2)	C8(3)	C9(4)
	6	

Table 7: Sixth Feature table

	C0(6)	
C1(7)	C2(8)	C3(9)
C4(0)	C5(1)	C6(2)
C7(3)	C8(4)	C9(5)
	7	

Table 8: Seventh Feature table

	C0(7)	
C1(8)	C2(9)	C3(0)
C4(1)	C5(2)	C6(3)
C7(4)	C8(5)	C9(6)
	8	

Table 9: Eight Feature table

	C0(8)	
C1(9)	C2(0)	C3(1)
C4(2)	C5(3)	C6(4)
C7(5)	C8(6)	C9(7)

	9	

Table 10: Ninth Feature table

	C0(9)	
C1(0)	C2(1)	C3(2)
C4(3)	C5(4)	C6(5)
C7(6)	C8(7)	C9(8)
	10	

Table 11: Tenth Feature table

E. PIN Entry Mechanism in Color Pass:

In this scheme, the user chosen PIN is of four colors. During the login session, when the Feature Tables appear in the screen then the login system gives some challenge values to the user. The challenge is passed through a secured media and so only the user can access it. In color pass technique, the user receives the challenge value through a headphone. Challenge values range from 1 to 10. Based on the challenge value the user will select the corresponding Feature Table. For example, challenge value 7 indicates that the user has to look in the seventh Feature Table. User will receive challenge value corresponding to each color of his PIN. After listening to each challenge value, user selects a Feature Table. Then with respect to the chosen color PIN,user locates the color cell in that table. The user then finds the value in that color cell and enters that value as response to the challenge. Similarly user has to 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.

Color Index	Assigned Values	Assigned colors
C0	0	Yellow
C1	1	Pink
C2	2	White
C3	3	Violet
C4	4	Dark Green
C5	5	Orange
C6	6	Sky
C7	7	Grey
C8	8	Dark Blue
C9	9	Green-Yellow

Table 12: Used colors for feature tables.

Each color has been assigned a number from 0 to 9 by the system as shown in above table. If user chooses four colors (say) C6C3C5C1, the system database stores user PIN as 6351. We have stored this user PIN in an array UCOL (indexed from 0 to 3). The four random numbers (challenge values) generated by system are 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 for generating user response.

User choosen color	Challenge	Response
C2	5	6
C3	7	9
C4	2	5
C1	5	5

Table 13: User Response table for a given challenge

Suppose user has chosen PIN C6C3C5C1 and he gets the challenge values 5, 7, 3, 5. So first user will go to the 5th 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 above table.

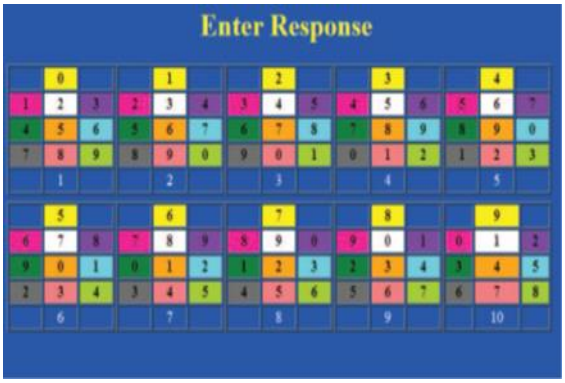

Fig. 1: User Interface on screen

Fig. 2: User interface for entering response

F. User Interface for Color Pass:

While implementing user interface we have assigned unique colors to each Ci (i varies from 0 to 9). Ten colors is chosen in such a way so that each color is clearly distinguishable from other. The actual interface is shown in Fig1. As the color cell's position in each table is fixed so user can locate the desired colored cell quickly. It is advantage for getting faster login time. The tables are designed in such a way so that the user interface does not look too elegant and also the space is used in an optimum manner. Similarities between keypads in Color Pass, as shown in Fig2 and classical PIN entry method makes our methodology more user friendly and easy to use for novice users. Only the two extreme keys at the bottom row are kept unused. If user chooses Yellow Pink Violate Grey and receives challenge values 6 3 5 6 then seeing the interface in Fig1 user will enter 5 3 7 2 using the key board showing at Fig2.

IV. CONCLUSION

In this project they have proposed a technique 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 technique, the user remembers four colors as his PIN. The technique works on the framework of partially observable attacker model. From security point of view the scheme is robust against some possible attacks such as shoulder surfing, guessing password, 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 users.

REFERENCES

[1] Nilesh Chakraborty, Samrat Mondal "Color Pass: An intillegent user interface to resist shoulder surfing attack". Color Pass: An intelligent user interface to resist shoulder surfing attack Students' Technology Symposium (TechSym), IEEE , Pages: 13 - 18, 2014
[2] M. M. Group, "http://www.internetworldstats.com/stats.htm," June 2012.
[3] C. Herley, P. C. Oorschot, and A. S. Patrick, "Passwords: If we are so smart, why are we still using them?," in Financial Cryptography, pp. 230–237, 2009.
[4] www.webeopdia.com/term/s/shoulder−surfing.html (last access octeber,2013).
[5] A. Paivio, "Mind and its evaluation: A dual coding theoretical approach,"2006.
[6] 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.
[7] 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.
[8] 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, pp. 467–472, 2007.
[9] G. E. Blonder, "Graphical passwords. in lucent technologies, inc.,murray hill, nj, u. s. patent, ed. united states," June 1996.
[10] 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.

