Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.20 – 26

REVIEW ARTICLE

REVIEW ON COLOR PASSWORD TO RESIST SHOULDER SURFING ATTACK

Ms. K.Devika Rani Dhivya (Assistant Professor)* M.Sc.,M.Phil.,MBA., **S.Pavithra** ** IV M.Sc(SS)
Department of BCA&M.Sc(SS), Sri Krishna Arts and Science College, Kuniamuthur, CBE, TN, India
Email Id- mailtopavithra18@gmail.com, Email Id- devika58@gmail.com

Abstract- Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, both the text-based password schemes and graphical password schemes are not secure and efficient enough and not adopted. Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with colors to generate secure passwords for authentication. The user passwords can be used only once and every time a new password is generated. In this paper, the user propose an improved text-based shoulder surfing resistant graphical password scheme by using color PIN entry mechanism which are resistant to shoulder surfing. In the proposed scheme, the user can easily and efficiently log in into the system. This proposed work gives more security over the password from shoulder surfing and accidental log in.

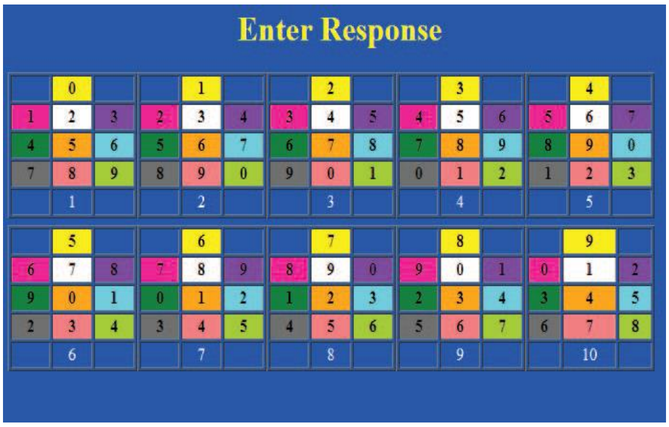
Keywords - Color PIN Entry Mechanism, Shoulder Surfing Attack, Texual Passwords, Graphical Passwords

I. INTRODUCTION

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]. color PIN is a widely famous mechanism for ease of usability, but it is prone to shoulder surfing attack [2] , in which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN.

Classical PIN-entry methods are vulnerable to a broad class of observation attacks (shoulder surfing, key-logging). A number of alternative PIN-entry methods that are based on human cognitive skills have been proposed. These methods can be classified into two classes regarding information available to a passive adversary: (i) the adversary fully observes the entire input and output of a PIN-entry procedure, and (ii) the adversary can only partially observe the input and/or output. In this paper we propose a novel PIN-entry scheme - Shoulder Surfing Safe Login (SSSL). SSSL is a challenge response protocol that allows a user to login securely in the presence of the adversary who can observe (via key-loggers, cameras) user input. This is accomplished by restricting the access to SSSL challenge values. Compared to existing solutions, SSSL is both user-friendly (not mentally demanding) and cost efficient. User usability study reveals that the average login time with SSSL is around 8 sec in a 5-digit PIN scenario. We also show the importance of considering side-channel timing attacks in the context of authentication schemes based on human cognitive skills.

The proposed color methodology implements one time pass paradigm. Thus corresponding to four color PIN's the user gets four challenges and enters four responses with respect to each challenge. The main target of color pass scheme is that it is very easy to use and does not require any special knowledge. Against shoulder surfing attack it also provides equal password strength as compared with the color PIN entry scheme.



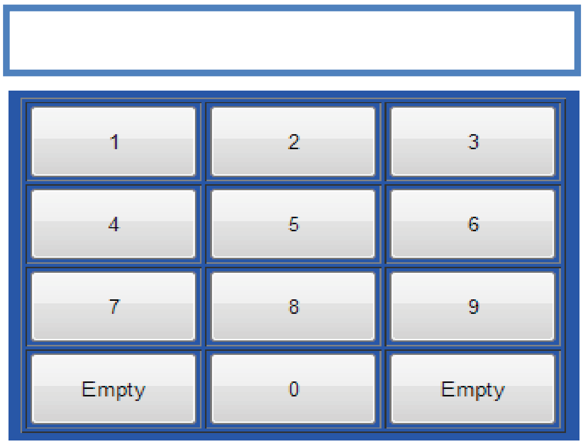
Enter Response

	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. Color Tables

This Fig.1 represents the nine color tables in which the user selects the color table according to the secret key generated through their hand held devices.



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

Fig.2. User Interface For Entering Response

Similarities between keypads in color password as shown in Fig.1.2 and classical pin entry method makes our methodology more user friendly. only the two extreme keys at the bottom row are kept unused. If the user chooses yellow pink green blue and receive values 8 3 6 4 then seeing the interface in Fig.1 user will enter 5 2 7 1 using the keyboard showing at Fig.2.

Objective

- The main objective of this project is to accomplish security.
- It is more efficient password system against attack like shoulder surfing or guessing the password.
- This scheme can be easily used by any type of user which widens the scope of applicability of our scheme.
- The session passwords provide better security against brute force attacks as password changes for every session.
- Usability, this scheme will be usable anywhere and at any time with a low error rate as well as a faster authentication result.
- Training, the system will provide users a simple and interesting training. They should not spend much time on training.
- The best use of human memory, the proposed scheme will benefit from the argument that people are better in recognizing images. Therefore, pass images should be easy to remember.
- Secure, the system will provide a strong line of defense against shoulder surfing brute force, intersection and educated guess attacks.

II. LITERATURE SURVEY

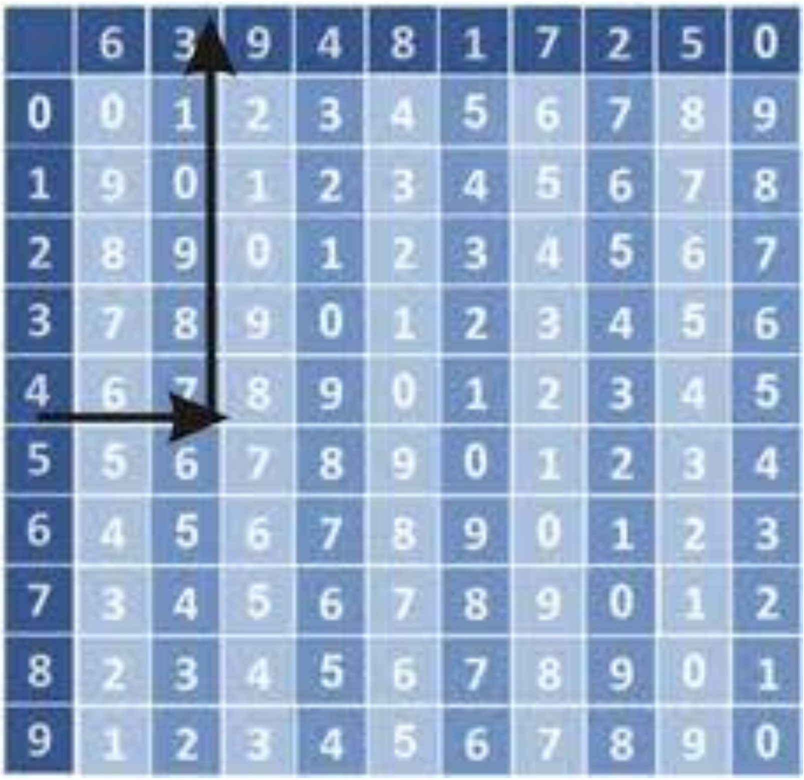
In 2002, to reduce the shoulder surfing attack, Sobrado and Birget [3] proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. But from all this schemes, the Movable Frame scheme and the Intersection scheme fail frequently in the process of Authentication. In the Triangle scheme, the user has to select and memorize several pass icons as his password. To login the system, the user has to correctly pass the predetermined number of challenges and in every challenge, the user has to find three pass-icons from a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons.

In 2009, To overcome the shoulder surfing attack, a graphical password scheme which uses color login and provide resistant to the shoulder surfing attack is proposed by Gao et al [4]. In this scheme the background color is a usable factor for reducing the login time. This Scheme has drawback like,the probability of accidental login of Color Login is too high and the password space is too small.

In 2012, a text based shoulder surfing resistant graphical password scheme, PPC is proposed by Rao et al [5]. 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. However, the login process of PPC is too complicated and tedious.

G.T.Wilfong [6] proposed a methodology where the user has to perform a simple mathematical operation. Where user remembers four digit PIN numbers and they will receive some values to their protected media. The user will add the corresponding values with that PIN numbers and perform a modulo 10 operation. Finally user will enter back the obtained digits using a public keyboard. Though this method is easy to execute for math oriented people and gives good security against guessing the password but became tedious to the non math oriented people and difficult to adopt.

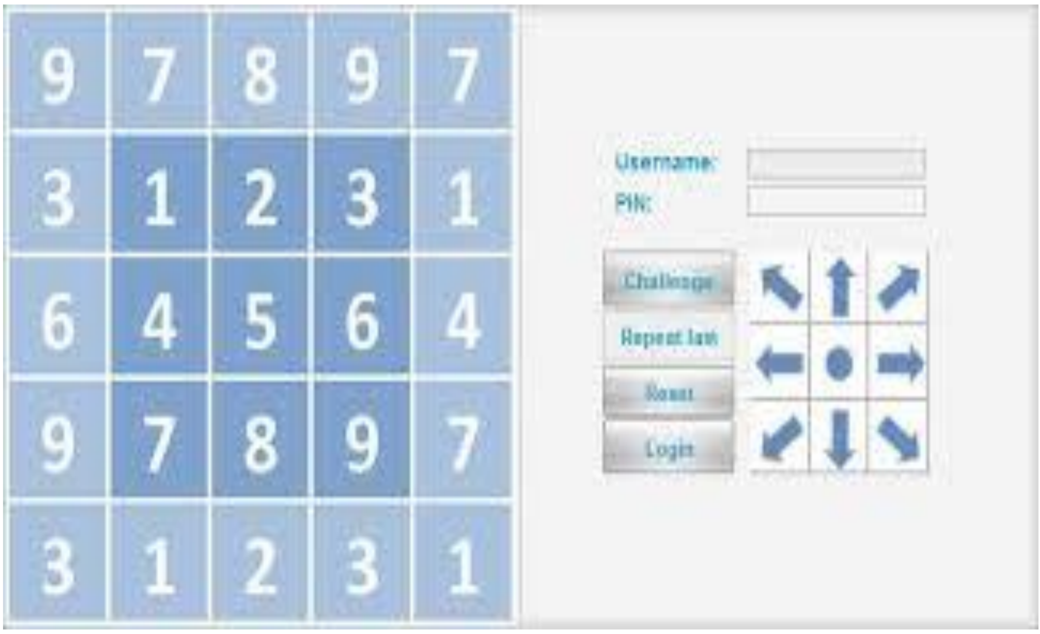
In this method Perkovic et al [7] proposed a concept of look up table.if the user PIN digit is 4 and the system generated value is 7 then the user first goes to the row number 4 in the look up table and subsequently goes to the digit 7 in that row. After that user will see the corresponding column number where 7 is placed and that column number will be enter back 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

Fig.3. Look Up Table

In shoulder surfing safe login, proposed by Perkovic et al [8] user does not provide any numbers instead of that they will be provided by the directions. Here the user remembers the five digit PIN numbers and the system throws values to the user with respect to the table and keypad consists of arrows. SSSL gives a robust solution to the shoulder surfing attack. 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.



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

Fig.4. Sssl Table

III. PROPOSED METHODOLOGY

The proposed Color Password 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 [9]. 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. Characteristics Of User Chosen Pin

In the existing system it is required to remember either few digits or few characters as users 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 and can choose one color more than once.

B. Steps For Login Procedure

- User enters his/her login id.
- Once system checks that the login id exists then it will generate the color tables.
- System then generates four random challenge values from 1 to 10.
- Next user will have to give response to those challenge values.
- Finally system will decide whether the user is legitimate or not.

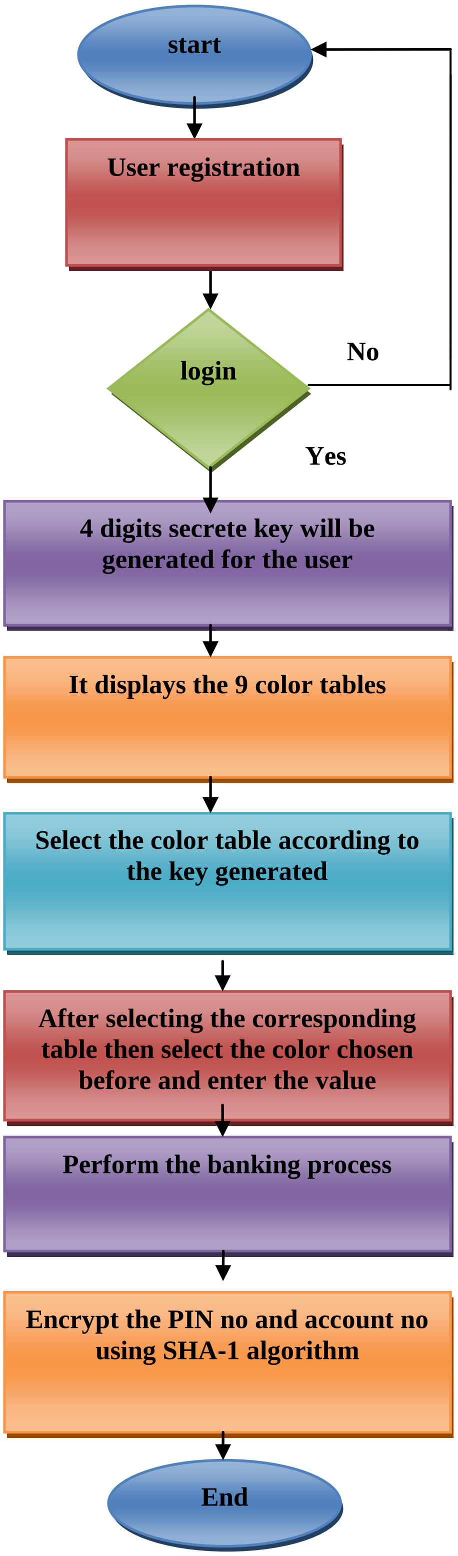

start
User registration
login
No
Yes
4 digits secrete key will be generated for the user
It displays the 9 color tables
Select the color table according to the key generated
After selecting the corresponding table then select the color chosen before and enter the value
Perform the banking process
Encrypt the PIN no and account no using SHA-1 algorithm
End

Fig5. Workflow Diagram of color password

C. Characteristics Of Color Tables

It consists of 10 different color table which are numbered from 1 to 10. In this table no color occupies in more than one cell. So for a particular table there will be ten different colors.

D. Pin Entry Mechanism in color password

In this scheme, the user chosen PIN is four colors. During login the color table appears in the screen then the system throws some values through handheld devices. That values are ranges from 1 to 10. Based on that value the user has to select the corresponding color table. This values will be randomly generated. Then corresponding to the chosen color PIN, user locates the color cell in that table. By locating the digit in that color cell user enters the digit. similarly user will respond to other three values and will finishes the login process. Valid response to the values will authenticate the user.

Color index	Assigned values	Assigned colors
C0	0	Yellow
C1	1	Pink
C2	2	White
C3	3	Violate
C4	4	Dark green
C5	5	Orange
C6	6	Sky blue
C7	7	Grey
C8	8	Peach puff
C9	9	Green yellow

Table I. Used Colors For Implementing Feature Tables

Each color has been assigned a number from 0 to 9 by the system as shown in Fig.5. 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).

E. Algorithm for Generating Tables

Rijndael (pronounced rain-dahl) algorithm is used to generate the color tables. The use of this Rijndael Algorithm in color password is to find the selected color from the nine color table and the value in this table should be matched with the value entered by the user in the user interface keypad. If matches the user can further perform the banking process. It that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES).

F. Algorithm for Encryption

MD5 which stands for Message Digest algorithm **5** is a widely used cryptographic hash function that was invented by Ronald Rivest in 1991. This algorithm is used to encrypt the user data such as Account No And Pin No. The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size “hash value” as the output. The input data can be of any size or length, but the output “hash value” size is always fixed.

IV. USER INTERFACE FOR COLOR PASSWORD

While implementing user interface we have assigned unique colors to each Ci (i varies from 0 to 9) (shown in TABLE.I). Ten colors is chosen in such a way so that each color is clearly distinguishable from other. The actual interface is shown in Fig. 1. 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 Pass, as shown in Fig.2 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 6 3 5 6 then seeing the interface in Fig.1 user will enter 5 3 7 2 using the key board showing at Fig.2.

V. 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. 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.
2. "www.webeopdia.com/terms/shoulder−surfing.html (last access october, 2013)."
3. L. Sobrado "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,2002
4. H. Gao, X. 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.
5. Schemes using text-graphical passwords," International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012.
6. 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.
7. T.Perkovic, M.Cagali, and N.Saxena, "Shoulder-surfing safe login in a partially observable attacker model," in Sion, R.(eds.) FC 2010. LNCS,pp. 351–358, 2010.
8. T. Perkovic, M. Cagali, and N. Rakic, "SSSL: Shoulder surfing safe login," in Software Telecommunications and Computer Networks, pp. 270–275, 2009.
9. "searchsecurity.techtarget.com/definition man-in-the-middle-attack (last access october, 2013)."