International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 3: March 2015, pp 23-25. www.aetsjournal.com ISSN (Online) : 2394-6237

Multi Color Pass Mechanism to Defend Against Shoulder Surfing Attack

Ramya.M, Hemalathaa.S, Jaya Anci.S.R ,Keerthana.M , Pavithra.S

Abstract— The traditional PIN entry mechanism is widely used for authentication. It is mainly used for authenticating user.It is widely used because of its usability and security. Eventhough it is considered as a secure method, it often leads to shoulder surfing attack, Here the unauthorized person may be fully or partially observe login session. This login session can be recorded and misused in future.In this paper we propose an intelligent user interface known as multicolor pass mechanism to defend against this problem. This is used to resist shoulder surfing attack so that only authorized user can login without revealing the actual PIN. It is based on partially observable attacker model. This multi color pass is safe for beginners.

Keywords— Color value, Shoulder Surfing Attack, User Interface ,Password, Partially Observable, lookup Table.

.

I. INTRODUCTION

There are a large number of Internet users around the world. Our software applications deal with sensitive as well as privateinformation 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 availableamong 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. 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. 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.

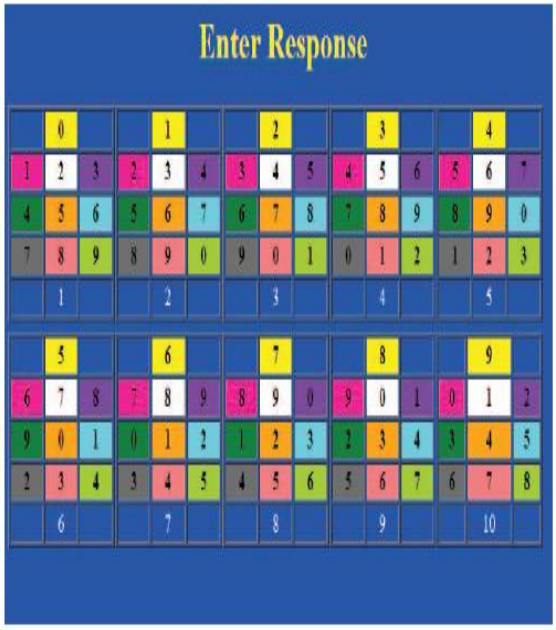

TABLE 1: Feature table

II. MULTICOLOR PASS METHODOLOGY

It implements one time pass paradigm. The user rate colors from 0 to 7 and it is remembered as 'RLYOBGIP'. During the login phase the use enters the username and account number. The color values from 0 to 7 are SMS via mobile phone. For each digit in the PIN number couple of colors will be displayed. According to the colors displayed, the user verifies the color values from SMS. Now the user finds the corresponding number from the lookup table which is generated randomly.

III. USER REGISTRATION

In the existing schemes it is necessary to recall either few digits or few alphabets as user PIN. But in Multi Color Pass

Ramya.M is Assistant Professor, Departmernt of Computer Science Engineering, Narasu's Sarathy Institute of Technology, Salem-636 305, Tamilnadu, India.

Hemalathaa.S, Jaya Anci.S.R ,Keerthana.M , Pavithra.S are UG Scholars (B.E – Computer Science and Engineering), Departmernt of Computer Science Engineering, Narasu's Sarathy Institute of Technology, Salem-636 305, Tamilnadu, India (e-mail: hemalathaa06@gmail.com, jayaanci@gmail.com).

scheme, combination of colors is used to create a PIN. Users have to choose four colors from a set of different colors which is represented as 0 to 7.Here the user is asked to enter values for each color from 0 to 7. Each colorrepresents a unique color (red, blue…). Since user chosen PIN is formed of four different colors the probability of guessing the PIN will be $1/10^{16}$.The phone number is registered by the user so that the color values can be sent as SMS via mobile phone.

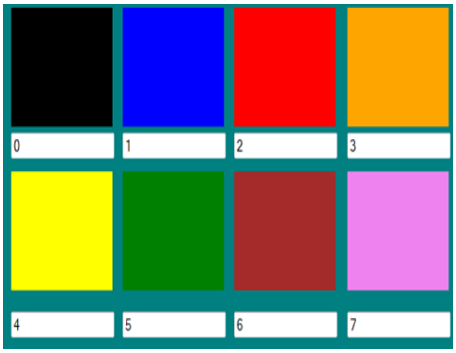

TABLE 2: Assigning values to colors

IV. Procedure For Login

The registered users can login using account number and username. Once the entered response is valid the color values are sent as SMS to the user.For instance, the SMS color values will be black=0, blue=1, and so on . The SMS will be sent to the mobile number which is entered during registration.

Black	0
Blue	1
Red	2
Orange	3
Yellow	4
Green	5
Maroon	6
Pink	7

TABLE 3: Received color values via SMS

V.Generation Of Lookup Table

The Lookup table consists of rows and columns. It resembles a matrix form. Here the values in the lookup table are randomly generated using Generic Algorithm. For each digit in the PIN number a couple of colors will be generated randomly. The corresponding color values are already known through SMS. According to the color values we find the values using lookup table. The first value of the color will be considered as row and second value as column.

For example, the values for randomly generated colors will be (6,0) (1,7) (5,2) (4,3). Using these values we find the equivalent value in the lookup table.

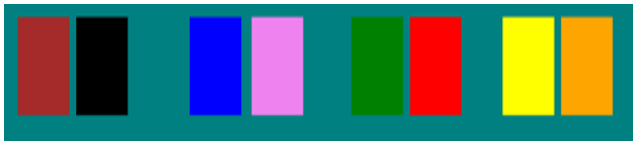

TABLE 4: Randomly generated colors

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

TABLE 5: Lookup Table

VI. RIJNDAEL ALGORITHM

To generate the look up table randomly, here we go for Mix Column operation by Rijndael Algorithm. In Mix Column function takes four bytes as input and four bytes as output. Matrix Multiplication is a combination of Multiplication and addition. Here multiplication by 1 means no change, multiplication by 2 means there is a shift to left, multiplication by 3 means there is a shift to left and XOR operation is performed for un shifted value.

VII. PIN ENTRY MECHANISM IN MULTI COLOR PASS

In Multicolor pass mechanism, the user will assign values for the colors.For each PIN number a couple of colors will be randomly generated. Throughout the login session, this randomly generated color will be visible. The color values are sent via mobile phones which helps the user to find the values from the look up table.

The color values vary from 0 to 7. Depending on the color values received, the user has to select the corressponding values from the look up table. For each digit in the PIN number user will receive two color values. The first value will be taken as row and the second value will be taken as column.Let the color value be 3 and 4 for the colors orange and yellow.Based on these values the user finds one number from that look up table.Look up table will be randomly generated using Rijndael Mix Column algorithm.Likewise the user will respond to the remaining color values and then completes the login session. Legalreply to the color values will validate the user.

VIII.USER INTERFACE FOR MULTOCOLOR PASS

Traditional PIN entry mechanism is more users friendly. Only two extreme keys at the bottom row are kept unused. The values got from the look up table will be entered in the user interface. Finally only four values will be entered.

TABLE 6: User Interface for Entering Response

IX. SECURITY ANALYSIS

As the scheme is partially observable the attacker cannot guess the color values. Llook up table is randomly generated and the values in the table are not static. So it is hard for the attacker to track the values in the look up table. This makes multi color pass robust against shoulder surfing attack. The probability of guessing the PIN number during the session is $1/10^{16}$.

Another possible attack is Side channel attack where the human users are involved. In this attack, the user tries to guess from the time the user executes a particular operation are the attack can record the users reaction time. In the proposed multi color pass scheme, the user response time is expected to improve. So each session the user gradually gets familiar and thus it improves the system response time. This makes the side channel attack quite challenging for the Multi Color Pass scheme.

X.CONCLUSION

In this paper we proposed a scheme to authenticate a user using a multiple color pins. This scheme is known as the multiple color pass scheme to provide an interface for users to login into the system. Using the matrix method, the four color pins are remembered by the user and given the responses in the interface. It is based on the partially observable attacker model. This method is quite forceful against shoulder surfing attack, guessing passwords, side channel attack etc… From usability point of view takes less time to login and it is user-friendly. It is used by both math and non-math oriented people. In future we will discover how to extend this model for fully observable attacker model.

ACKNOWLEDGMENT

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," June2012.
[2]"www.webeopdia.com/term/s/shoulder−surfing.html (last access octeber,2013)."
[3] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability ofgraphical passwords," International Journal of Network Security, vol. 7,no. 2, pp. 273–292, 2008.
[4] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistanttextual-graphical password authentication scheme,"
[5] G. E. Blonder, "Graphical passwords. in lucent technologies, inc.,murray hill, nj, u. s. patent, ed. united states," June 1996.
[6] T.Perkovic_, M.C" agalj, and N.Saxena, "Shouldr-surfing safe login in apartially observable attacker model," in Sion, R.(eds.) FC 2010. LNCS,pp. 351–358, 2010.access october, 2013)."
[7] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM Journal on Computing, vol. 15,pp. 364–383, may 1986.
[8] P. C. Kocher, "Timing attacks on implementations of diffie-hellman,rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1996.