International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

SHOULDER SURFING ATTACK PREVENTION USING COLOR PASS METHOD

Bagade Om , Sonawane Anuja , Patil Akash, Patil Yogita, Maurya Jagruti

Department of Computer Engineering
Shram sadhana trust's college of engineering & technology, Bambhori, Jalgaon 425001

Abstract—*The traditional PIN mechanism is mostly used for authentication. It is popular method due to its usability and security. Though it is secure method, it often leads to direct observational attack, such as human shoulder-surfing and camera based recording. In this paper proposed system provides implementation of color pass methods to defend against shoulder surfing attack. User can enter the session without revealing the actual PIN. It provide strong security against shoulder surfing attacks and have intelligent user interface.*

Key Words—Color PIN, User Interface, Lookup table, Shoulder surfing Attacks.

1. INTRODUCTION

In shoulder surfing attack, the amount of internet users has been reportable as approximately a pair of 4 billion worldwide, and from 2000 to 2015, it's a staggering 566.4%increase. This huge range of users consists of various genuine users and malicious users as well which try to access sensitive and private data of other users. So its necessary to provide protection to the system so that genuine and malicious users are often identified properly. In computer security, authentication is such a technique by that the system identifies the real users. Among several authentication schemes, password based authentication method is still one of the mostly accepted solution due to its ease of use and value effectiveness. Though conventional PIN entry mechanism is mostly famous due to its easy usability, however it's prone to shoulder surfing attack during which an attacker will record the login procedure of a user for an entire session and can retrieve the users original PIN. based on the knowledge available to the attacker, secure login ways are often classified into two broad classes as totally observable and partially observable. In the first class, the attacker will totally observe the whole login procedure for a particular session and in the second, the attacker will partially observe the login procedure. The proposed Color Pass methodology implements onetime pass method. In this method corresponding to four color PINs, the user gets four challenges and enters four responses with respect to every challenge. The great benefit of Color Pass scheme is that it's easy to use and doesn't need any pre-knowledge. In addition to the presentations against shoulder surfing attack, it also provides equal password strength which is better than the traditional PIN entry scheme.

2. LITURATURE SURVEY

L. Sobrado Graphical passwords, The Rutgers Scholar, an Electronic Bulletin for Undergraduate analysis proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme [6]. To overcome the drawbacks of Sobrado and Birgets scheme, the Convex Hull Click (CHC) is proposed by Wiedenbeck et al., 'Design and analysis of a shoulder-sarong resistant graphical password scheme'. Improved version of Triangle scheme with great security and usability [5]. Convex-Hull Click scheme has long login time. 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 [1]. Design and analysis of a graphical password scheme. Background color could be a usable factor for reducing the login time. A text-based shoulder surfing resistant graphical password scheme in which the user has got to find his textual password and so follow a

special rule to mix his textual password to get a session password to login the system is proposed by H. Zhao and X. Li [2], S3PAS: A scalable shoulder-sarong resistant textual graphical password authentication scheme. A text-based shoulder surfing resistant graphical password scheme by using colors is proposed by Sreelatha et al. 'M. Sreelatha, M. Anirudh, Md. grand Turk Ahamer, and V. Manoj Kumar [3]. Authentication schemes for session passwords using color and images, International Journal of Network Security & Its applications'. Clearly, as the user has got to additionally study the order of many colours, the memory burden of the user is high. To avoid the above drawbacks we'll describe a straightforward and efficient technique for the shoulder surfing Attack using Texts and color primarily based graphical password scheme [4], it uses ten decimal numbers.

3. EXISTING SYSTEM

Shoulder surfing attacks are not new. In literature, we find many graphics based techniques to prevent such shoulder surfing attacks. However, we will discuss here a number of the partially observable schemes to propose the color Pass scheme. It includes number of various techniques like Movable Frame theme, the Intersection theme, the triangle theme, convex Hull Click theme (CHC), graphical password scheme that uses color login but generally there's possibility of password recognized by the third person or hacker. The problem is password isn't protected by the existing techniques. The proposed solution is somewhat more efficient than the existing ones. Colorpass strategies are comparatively new fields of password preventions that are being explored for advancement within the existing preventive techniques. The colorpass strategies makes use of the concept of entering the PIN ofuser without revealing the actual PIN and hence prevent from shoulder surfing attacks.

4. PROPOSED SYSTEM

A. System architecture:

The proposed system is based on observable attacker model, In this attacker cannot identify the actual pin of the user but attacker can only see the response values entered by the user which are different than the original pin. Thus it's assumed that user gets the challenge digits for ensuring security against man-in-middle attack. This all replicated through the four methods as follows:

1. Mod ten table method.

2. Shoulder surfing Safe Login method.

3. BW method.

4. Color pass method.

The general architecture of proposed system is as shown in following figure 4.1. Which takes input as account no if user has already registered otherwise he has to register first by entering all the information. After selecting the method which user wants he has to enter account number and the challenge digit which is automatically generated by selected method. According to challenge digit generated user will enter response value and then user will login to the system as an output of the proposed system.

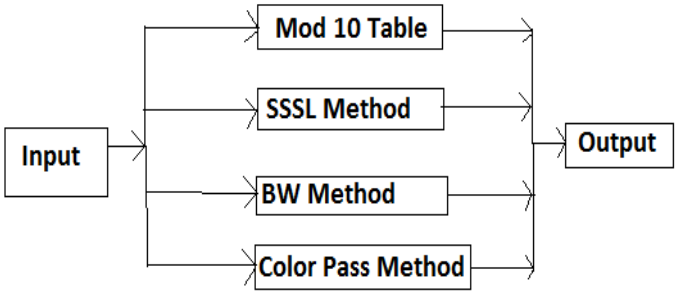

Figure 4.1: General System architecture

1.1 System architecture of MOD10 table Method:

Figure 4.2 describes architecture of Mod ten table method. In Mod ten table method, firstly user enters his account number which is already stored in database. Then system generates challenge digits. After that, system generates MOD10 table from which user can enter correct look up value. Finally user will login the system.

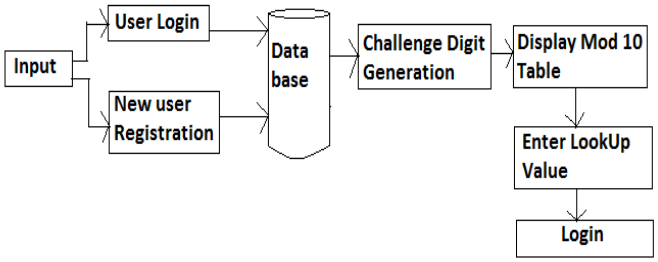

Figure 4.2: System architecture of MOD10 table method

1.2 System architecture of SSSL:

Figure 4.3 describes architecture of SSSL method. In SSSL method firstly user enters his account number which is already stored in database. Then system generates challenge digits randomly. After that, table for orientation of digit and the computer keyboard structure for SSSL method display on screen. From which user calculate his response digits and press appropriate directions with respect to table. Finally user login the system.

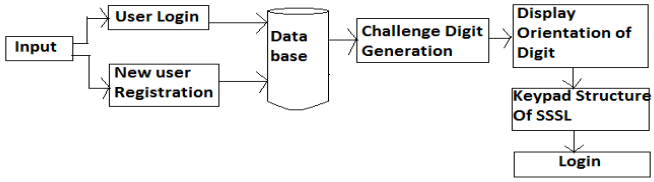

Figure 4.3: System architecture of SSSL method

1.3 System architecture of Black and White Method:

Figure 4.4 describes architecture of Black and White method (BW). In BW method, firstly user enters his account number which is already stored in database. Then system generates challenge digits. After that, color boundary table is displayed from boundary table user enters proper color according to challenge digits. Finally user login the system.

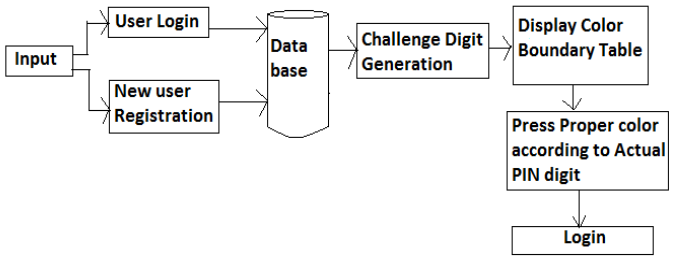

Figure 4.4: System architecture of BW method

1.4 System architecture of Colorpass Method:

Figure 4.5 describes architecture of Color pass method. In colorpass method, firstly user enters his account number which is already stored in database. Then system generates challenge digits. After that, compare actual PIN predefined color table. Find no corresponding to that color in feature table. Then users enter the number on the respected color as his response value. Finally user login the system.

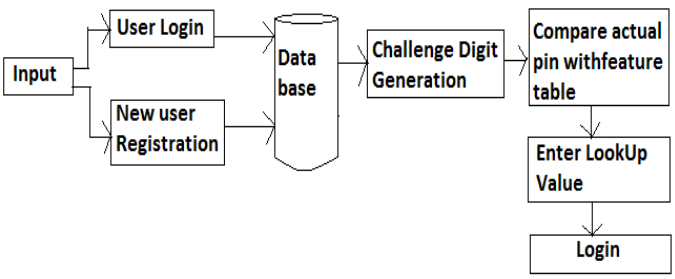

Figure 4.5: System architecture of Colorpass Method.

B. METHODOLOGY:

1.1 Mod 10 table method :

In this technique Perkovic proposed a concept of lookup table. If user selected PIN digit is nine and also the system generated challenge is six then the user looks in the row number six in the lookup table i.e. (Figure 4.6) and afterwards user finds the digit nine in that row i.e. in sixth row after that user can see for the respective column number where nine is placed (here one) and enter back 1 as response corresponding to the one challenge. If the digits in the top row of table are arranged in ascending order from zero to nine then it'll be equivalent as modulo ten additions. Hence the name of the table is justified. But one of the drawbacks of this method is login time during this method login time goes high with respect to modulo ten technique.

	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 4.6: User Lookup table

1.2 SSSL Method:

In SSSL method user does not need to provide numbers as response instead of user enters some directions as response to the system. In this scheme user has to remember four digits PIN number. In orders to authenticate themselves the user needs to response to the challenge values shown to them with respect to the orientation table and arrow keyboard shown in Fig. 4.7 the table in SSSL method created in such a way that each digit i is a neighbour to alternative eight digits from the set 1, 2 ...9 (see Fig. 4.7[a] i.e. Orientation of digits). User find the relative position of their original PIN digits and therefore the challenge values via keyboard shown in (Fig. 4.7[b] i.e. keyboard structure for SSSL) the subsequent example will provides a clear plan regarding SSSL methodology. For Example, Suppose the actual password of user is 3895 and the challenge digit generated by the system is 1278. The digit 1 is placed left side to the 1 in Fig. 4.7[a] so that the user press the left side arrow. Again actual PIN digit is 8 and challenge digit is 2 then press up arrow. When challenge digit and actual PIN are same then press self arrow.

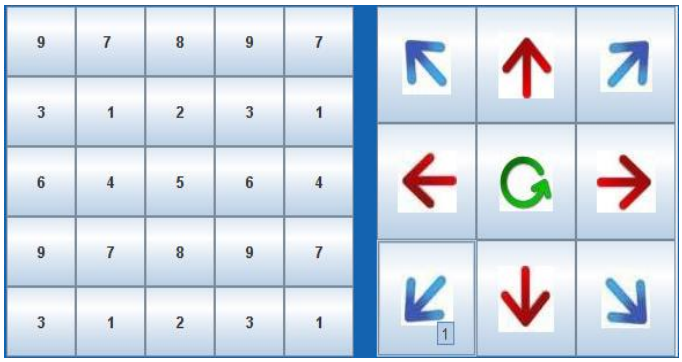

Fig. 4.7: (a) Orientation of digits (b) Keypad structure for SSSL

1.3 BW Method:

We study the BW technique more and acquire the subsequent results, each by experimentation and on paper, regarding the scheme. The shoulder-surfing resilient versions hold severe round redundancy, and this can be exploited by adversaries. The black and white key presses throughout PIN entries are unbalanced, and this can be exploited by the adversaries.

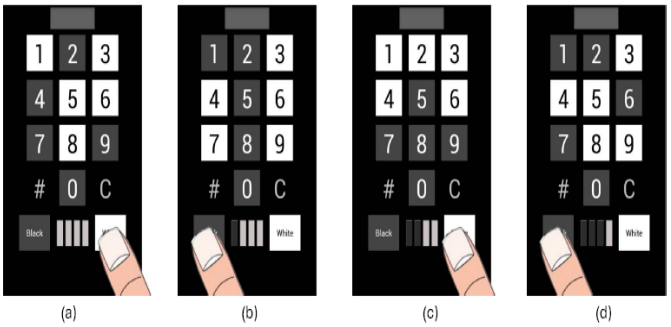

Fig. 4.8: BW method

1.4 PIN Entry Mechanism in Color Pass:

In this scheme, the user chosen PIN is four colors. Throughout the login procedure, when the Feature Tables seem inside the screen then the system throws some challenge values to the user. Challenge values vary from 1 to 10. Supported the challenge worth the user has got to pick the corresponding Feature Table. As an example, challenge value four indicates that the user possesses to seem inside the Fourth Feature Table. User will receive challenge corresponding to every color of his PIN. The challenge values generates randomly by the system. Once getting each challenge value, user selects a Feature Table. Then corresponding to the chosen color PIN, he locates the color cell in that table. The user then finds the digit therein color cell and enters that digit as response to the challenge. Equally user will reply to the other three challenge values and may complete the login method. Valid response to the challenge values will authenticate the user.

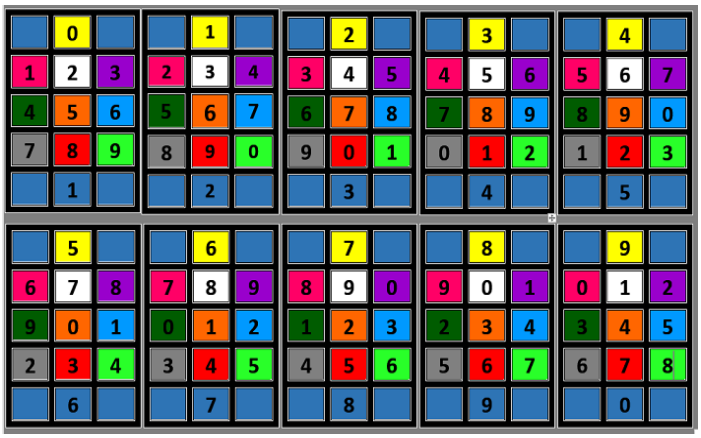

Fig. 4.9: User Interface On Screen

0	Yellow
1	Pink
2	White
3	Violet
4	Dark Green
5	Orange
6	Sky Blue
7	Grey
8	Red
9	Light Green

Fig. 4.10: Used colors for implementing feature tables

For example, suppose actual PIN is 1,2,3,4 then first user look at in fig. 4.10 and conform the respective predefined colors then system generates the challenge digit. Suppose challenge digit is 6,7,8,9. After that, user selects the feature table Fig. 4.9 with respect to its challenge digits. Then the user gives the response value with respect to challenge digit and color to the system and user gets login.

C. ALGORITHMS:[4]

Algorithm for color pass method:

Algorithm 1 :Generating tables in Color Pass

Input: This algorithm can 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 can take array UCOL, array CLICK and array RAN as input.

Output: This algorithm can update value of array EVAL by one 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 can take array EVAL as input after executing algorithm two.

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

5. RESULT:

SSAPCM is used to prevent attackers to see the password while entering from behind. It is used for the security purpose of owners account. In this we implement four methods that Pare

1. Mod10 method
2. SSSL method
3. Color Pass Method
4. BW method

In this system, user's information is stored in Mysql database which is shown in Fig. 5.1. This database contain all the user's detail which is required for registration.

	AccountNo	PinNo	FullName	Balance
	123456789000	1111	aakash patil	656767
	1234567899	5678	Yogita Patil	1234
	8275389513	1111	sham patil	777
	827538957012	4321	snehal patil	800
	940455167612	1111	aashu suryavanshi	444
	940455167812	1111	bhushan patil	555
	9420788677	1111	aasha patil	111

Figure 5.1: User database

Then user will select one of the method for login procedure and then they enter their account number such that 123456789012 after that system will generate a challenge digit randomly such as 3344 for above account number. Original pin is remembered by the user itself suppose it is 1234.Using that challenge digit and original pin user will perform calculation and get response value which they enter as their original pin and calculation is different for every method. After that user will safely login to the system. These methods provide security in their own way and thus differ from each other. From result, we compare four methods based on two parameters that are time complexity and user friendliness. The result of comparison is shown in below table 5.1.

Table 5.1: Comparison between Method

Methods	Time Consumption	User Friendliness
Mod 10 Table method	Less	More
SSSL Method	More	Less
Colorpass Method	Less	Less
BW Method	Less	More

6. CONCLUSION:

Proposed system will implementing color pass mechanism for shoulder surfing attacks. In this color pass mechanism four methods that are SSSL, BW, Mod10 table & color pass are implemented to prevent shoulder surfing attacks. It provides an intelligent interface for users to login into system in a public domain. From security point of view these different methods are 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.

7. REFERENCES

[1] R. Dai, and H. Gao, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on Innovative Computing, data and control, pages 675678, December 2009.

[2] X. Li, and H. Zhao, "S3pas: A {scalable shoulder-sur_ng resistant textual-graphical password authentication scheme," Proc. of 21st Int. Conf. on Advanced information Networking and Applications Workshops, 2:467472, May 2007.

[3] M. Anirudh, and M. Sreelatha, "Authentication schemes for session passwords using color and images," International Journal of Network Security and Its Applications, 3(3), May 2011.

[4] Samrat Mondal, and Nilesh Chakraborty, "Color pass: an intelligent user interface to resist shoulder surfing attack," IEEE, 2014.

[5] J. Birget, and S. Wiedenbeck, "design and analysis of a shoulder-surfing resistant graphical password scheme," proc. of working conf. on advanced visual interfaces. IEEE, pages 177{184, May 2006 }.

[6] L. Sobrado, and Graphical passwords, "the rutgers scholar, an electronic bulletin for undergraduate analysis," IEEE, 4, 2002.

[7] Jin Hong, and Taekyoung Kwon, "Analysis and improvement of a pin entry method resilient to shoulder-surfing and recording attacks," IEEE, 10(2), february 2015.