IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Intelligent Techniques with GUI by Challenge Keypad for Secure Password

Krishna S. Gaikwad[1], Prof. Amruta Amune[2]

Department of Computer Engineering, G. H. Raisoni College of Engineering, Ahmednagar[1, 2]

Abstract: In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. This problem has come up with a new solution. Devising a user authentication scheme based on personal identification numbers (PINs) that is both secure and practically usable is a challenging problem. The greatest difficulty lies with the susceptibility of the PIN entry process to direct observational attacks, such as human shoulder-surfing and camera-based recording.PIN entry mechanism is widely used for authenticating a user. It is a popular scheme because it nicely balances the usability and security aspects of a system. However, if this scheme is to be used in a public system then the scheme may suffer from shoulder surfing attack. In this attack, an unauthorized user can fully or partially observe the login session. Even the activities of the login session can be recorded which the attacker can use it later to get the actual PIN. In this paper, we propose an intelligent user interface, known as Color Pass to resist the shoulder surfing attack so that any genuine user can enter the session PIN without disclosing the actual PIN. The Color Pass is based on a partially observable attacker model. The experimental analysis shows that the Color Pass interface is safe and easy to use even for novice users.

Keywords: PIN, Shoulder Surfing Attack, User Interface, Partially Observable.

I. INTRODUCTION

In a recent report [1], the number of Internet users has been reported as approximately 2.4 billion worldwide, and from 2000 to 2012, it is a staggering 566.4% increase. This huge number of users consists of both genuine users and malicious users. So software applications which deal with sensitive and private information must provide a sound protection to the system so that genuine and malicious users can be identified properly. 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 [2]. Though conventional PIN entry mechanism is widely famous for ease of usability, but it is prone to shoulder surfing attack [3] in which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN.

Based on the information available to the attacker, secure login methods can be classified into two broad 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 procedure. Our proposed 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. The main objective of Color Pass scheme is that it is easy to use and does not require any special prerequisite knowledge. In addition to the resistance against shoulder surfing attack, it also provides equal password strength as compared with the conventional PIN entry scheme. The rest of the paper is organized as follows- Section II is about some existing methodologies proposed for partially observable system. In Section III, the proposed Color Pass scheme has been discussed in detail. The user interface for Color Pass has been described in Section IV. Some of the important features and usability analysis of Color Pass have been illustrated in Section V. Finally we conclude in Section VI and give future direction of our work.

II. RELATED WORK

Shoulder surfing attack is not new. In literature, we find many graphics based techniques [4] [5] [6] [7] [8] to resist such attacks. However, we will discuss here some of the partially observable schemes which have motivated us to propose the Color Pass scheme.

A. Mod 10 method

In this work G.T Wilfong [9] proposed a methodology where user has to perform a simple mathematical operation. User remembers a four digit PIN number from the set {0, 1,..., 9}. User receives a challenge from the set {0, 1,..., 9} via a protected media. User will add the challenge digit with the corresponding PIN digit and will perform a modulo10 operation. Finally he will enter back the obtained digit using a public keyboard. Suppose the first digit of the user chosen PIN is 5. User now securely receives a challenge 7 from the system. So the valid response by user will be (5+7) modulo 10 (which is equal to 2). Though this method is easy to execute for math oriented people and gives good security against guessing the password but for non-math-oriented people this methodology is difficult to adopt.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

B. Mod 10 table method:

In this method Perkovicet.al. [10] Proposed a concept of lookup table. If user chosen PIN digit is 5 and the system generated challenge is 7 then the user first goes to the row number 5 in the lookup table and subsequently goes to the digit 7 in that row. After that user will see the corresponding

TABLE I: User Lookup Table

	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

TABLE II: User response table of SSSL

PIN	Challenge	Response
9	3	↓
6	6	◦
9	5	
7	7	◦
8	1	

Column number where 7 is placed (here 9) and enter back 9 as response corresponding to the first challenge.

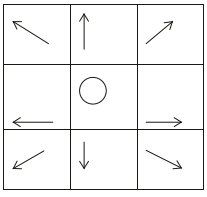
If the digits in the top row of Table I is arranged in ascending order from 0 to 9 then it will be equivalent as modulo 10 addition. Hence the name of the table is justified. But one of the drawback of this procedure is login time in this method goes high with respect to modulo 10 method. The other drawback we observed that the error rate does not improve much with the number of attempts.

C. Shoulder Surfing Safe login

Unlike the previous two schemes, in SSSL, proposed by Perkovic et al. [11], user does not provide any number as response rather enters some direction to the system.

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

(a)



(b)

Fig. 1: (a) Orientation of digits (b) Keypad structure for SSSL

In this scheme a user remembers five digits PIN. In terms of authenticate himself the user has to answer to the challenge values throws to him with respect to the table and keypad consist of arrows shown in Fig.1. The table in SSSL method constructed in such a way that every digit iis an immediate neighbor to other 8 digits from the set {1, 2… 9} (see Fig.1 (a)). User locate the relative position of their original PIN digits and the challenge values via keypad shown in Fig.1 (b). The following example will give a clear idea about SSSL methodology.

Suppose user chosen a five digit pin 96978, and the corresponding challenge value is 36571. As digit 3 is placed under the value 9 in Fig.1 (a) so the user will press the down arrow. When the PIN digit is 6 and the challenge is also 6 then the response is press ◦ key. The valid responses is shown in TABLE II which is clearly understandable from Fig.1 (a). SSSL gives a robust solution to the shoulder surfing attack. Also the scheme is easy for non-math oriented users. 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.

III.PROPOSED METHODOLOGY

The proposed Color Pass 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 [12]. 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.

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 $\{C_0, C_2,\cdots,C_9\}$. 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 Ci 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 $1/10^4$.

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 <Ci,Vi>. Here Ci denotes the color of the cell iand Viindicates the digit corresponding to cell i.

Ci 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 positions of color cells is shown in Table III 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 III: Identifying Each Cells in k^{th}table

All cells in a table also contain a unique value Vi from the set {0,1,...,9}. Another important characteristics is that in each cell i, the pair <Ci,Vi>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.

In this scheme, the user chosen PIN is four colors. During the login procedure, when the Feature Tables appear in the screen then the system throws some challenge values to the user. The challenge is passed via a secured media and so only the user can access it. In our scheme, the user can receive the challenge via a headphone.

Challenge values range from 1 to 10. Based on the challenge value the user has to select the corresponding Feature Table. For example, challenge value 4 indicates that the user has to look in the Fourth Feature Table. The challenge values will be generated using pseudo-random function [13]. User will receive challenge corresponding to each color of his PIN.

After listening to 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 in that color cell and enters that digit as response to the challenge. Similarly user will 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
C_0	0	Yellow
C_1	1	Pink
C_2	2	White
C_3	3	Violate
C_4	4	Dark Green
C_5	5	Orange
C_6	6	Sky
C_7	7	Grey
C_8	8	Peach Puff
C_9	9	Green Yellow

TABLE IV: Used colors for implementing feature tables

Each color has been assigned a number from 0 to 9 by the system as shown in TABLE IV. If user chooses four colors (say) $C_2C_3C_4C_1$, the system database stores user PIN as 2341.

IV. 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] M. M. Group, "http://www.internetworldstats.com/stats.htm," June 2012.
[2] 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.
[3] "www.webeopdia.com/term/s/shoulder−surfing.html (last access octeber, 2013)."
[4] A. Paivio, "Mind and its evaluation: A dual coding theoretical approach," 2006.
[5] 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.
[6] 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. 12, pp. 102–127, 2005.
[7] 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.
[8] G. E. Blonder, "Graphical passwords. in lucent technologies, inc., murray hill, nj, u. s. patent, ed. united states," June 1996.
[9] 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.
[10] T.Perkovic, M.Cagalj, and N.Saxena, "Shouldr-surfing safe login in a″ partially observable attacker model," in Sion, R.(eds.) FC 2010. LNCS, pp. 351–358, 2010.
[11] T. Perkovic, M. Cagali, and N. Rakic, "SSSL: Shoulder surfing safe login," in Software Telecommunications and Computer Networks, pp. 270–275, 2009.
[12] "searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last access october, 2013)."
[13] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM Journal on Computing, vol. 15, pp. 364–383, may 1986.

DOI 10.17148/IJARCCE.2015.411108