Color Code: A Model to Refuse the Shoulder Surfing Attack

Yogesh Bhadale
Yogesh9363@gmail.com

Gaikwad Shweta
shwetagaikwas048@gmail.com

Narke Prajakta
prajaktanarke98@gmail.com

Prof.Kothawale G.S.
Ganesh.kothawale@gmail.com

Student,Computer Engineering,AAEMFS COE,Maharashtra,India
[2] Student,Computer Engineering,AAEMFS COE,Maharashtra,India
[3] Student,Computer Engineering,AAEMFS COE,Maharashtra,India
[4] Professor,Computer Engineering,AAEMFS COE,Maharashtra,India

Abstract:- *For authentication users mainly use PIN entry mechanism. Traditional password-based authentication schemes are vulnerable to shoulder-surfing attacks.But one of the drawback of this scheme is that it suffers from shoulder surfing attack.An unauthorized user can fully or partially observe the login session in this attack. To get the actual PIN the attacker can record the activities of the login session and can use it later. In this paper,it 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.*

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

1.INTRODUCTION:

Now Day's most of the people used net banking,online transaction or ATM transaction.And uses of online transaction is increasing rapidly. This huge number of users consists of both genuine users and malicious users. So software applications which deal with sensitive, private and secret information, must provide a sound protection to the system so that genuine and malicious users can be identified properly.In computer security have a different types of authentication shcemes like password authentication captcha for identify the genuine user. Password based authentication is still one of the widely accepted solution for its ease of use and cost effectiveness.The typical PIN entry system is famous in world wide for easy usability.But it causes to shoulder surfing attack ,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 categoriesfully
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 erequisite 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 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 . 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

2.LITERATURE SURVEY

In 2002, to reduce the shoulder surfing attack, Sobrado and Birget 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 riangle 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. 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.

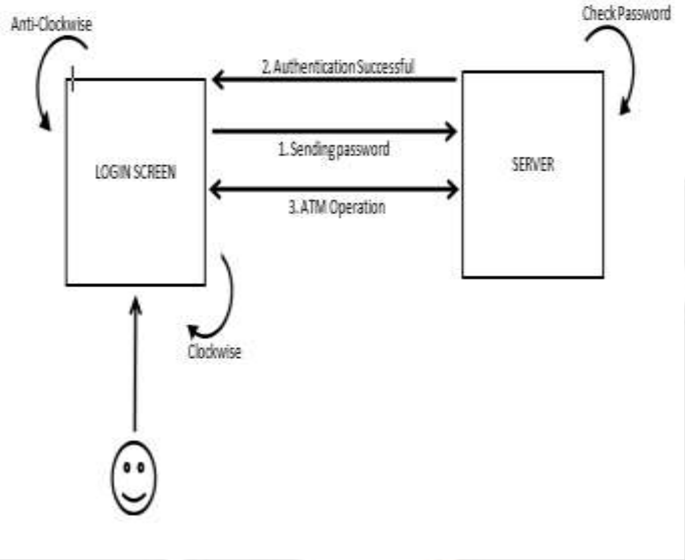
In 2012, a text based shoulder surfing resistant graphical password scheme, PPC is proposed by Raoet al To login the system, the user has to mix his textual password to produce several pass pairs, and then follow four predefined rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious G.T.Wilfong 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 wit 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 all 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

3.PROBLEM STATEMENT

This system focus on developing security which can remove shoulder surfing attack and provide better authentication using color pass algorithm. 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.

4. ARCHITECTURE

Color code 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. 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 {C0,C2, ・ ・ ・ , C9}. User has the flexibility to choose one color more than once. So one possible instance of user chosen PIN might
be C1C2C1C4. 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 1/104.

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. 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).

Security Analysis

As the scheme is partially observable so the attacker cannot see the challenge values received by the user. Only the responses by the user are visible to the attacker. Thus to ensure security, the attacker should not able to guess the PIN just by seeing the responses. Suppose user has chosen color C5 as one of his secrete PIN and he gets a challenge 4 corresponding to that PIN digit. So a valid response from user will be 8 as per the Feature Tables described earlier. Now as attacker does not know the challenge value 4 and as digit 8 is printed upon all ten colors of all ten tables so attacker will not be able to retrieve the original color chosen by user. This makes Color Pass robust against shoulder surfing attack.

In terms of guessing attack, it has equal strength compared to a 4 digit PIN scheme. The probability of guessing during a session is 1/104 as for each color there are ten possibilities. The co-relation between user chosen color can not be guessed by an attacker which is an obvious advantage of Color Pass over SSSL.

6.CONCLUSIONS

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.

8.REFERENCE

[1]M.M.Group,http://www.internetworldstats.com/stats.htm," June2012.

[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. 1-2, 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.C˝ agalj, 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.

[14] P. C. Kocher, "Timing attacks on implementations of diffie-hellman,rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1996.

[15] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in ACM Conference on Computer and Communications Security, pp. 373–382, 2005.