ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Smart User Interface to Prevent Shoulder Surfing Attack Using Color Code

Yathiraj GR[#1], Santosh VG[#2], Sushma KR[*3], Muthappa KU[#4]

Assistant Professor, Dept. of Computer Science, Coorg Institute of Technology, Ponnampet, Kodagu, Karnataka, India [#1]

Assistant Professor, Dept. of Computer Science, Coorg Institute of Technology, Ponnampet, Kodagu, Karnataka, India [*2]

Assistant Professor, Dept. of Computer Science, Coorg Institute of Technology, Ponnampet, Kodagu, Karnataka, India [*3]

Assistant Professor, Dept. of Computer Science, Coorg Institute of Technology, Ponnampet, Kodagu, Karnataka, India [#4]

ABSTRACT : Classical PIN entry mechanism is broadly used for authenticating a user. It is a popular scheme because it properly balances the usability and safety aspects of a organism. However ,if this scheme is to be used in a public system then the design might endure since accept surfing attack. In this attack, an unauthorized user can completely or partially watch the login session .Even the activities of the login gathering can be recorded which the attacker can use it soon after to get the actual PIN. In this paper ,we suggest an intelligent user interface, known as Color Pass to oppose the accept surfing attack so that any authentic user can enter the session PIN without disclosing the authentic PIN. The Color Pass is based on a partially noticeable attacker model. The experimental analysis shows that the Color Pass interface is secure and simple to use even for novice users.

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

I. INTRODUCTION

In a recent report [1], the number of Internet users has been reported as around 2.4 billion world wide, and from 2000 to 2012, it is a staggering 566.4% increase. This huge number of users consists of both valid users and malevolent users. So software applications which deal with sensitive and personal information, must supply a sound

protection to the system so that authentic and malicious users can be recognized accurately. In computer security, authentication is such a method by which the system identifies the authentic users. Among several authentication schemes, password based authentication is still one of the broadly established solution for its ease of use and cost effectiveness [2]. Though conventional PIN entry mechanism is broadly renowned 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 whole session and can get back the user original PIN.

Based on the information available to the attacker, secure login methods can be classified into two broad categories completely observable and partially observable. In the first one, the attacker can completely observe the whole login procedure for a particular session and in the second one, the attacker can partially watch the login procedure. Our proposed methodology falls into second category and users are compulsory to remember four colors instead of conventional four digit PINs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

II. PROPOSED METHODOLOGY

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 potency 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.

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 known by the user. Thus it is not mentioned that the media through which user get the challenge should ensure security next to man-in-middle attack. In this section we first discuss about the characteristic of user chosen PIN followed by user login process 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.

While implement user interface we have assigned unique colors to each (i varies from 0 to 9) (shown in TABLE XIV). Ten colors is chosen in such a way so that each color is clearly distinguishable from other. The actual interface. 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. similarity flanked by keypads in Color Pass, as shown in 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 user will enter 5 3 7 2 using the key board showing at.

III. SECURITY AND EVALUATION STUDY OF COLOR PASS

Some of the salient features of the proposed Color Pass scheme is described in the followings. Mainly two broad aspects - security and usability are discussed next.

3.1 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 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.
Side channel attack is another possible attack where human users are concerned. Some variation of this attack is found in. In this attack, the attacker tries to guess from the time the user takes to execute a particular operation. If the attacker can record the user's reaction time, then SSSL is sensitive for such an attack. In the proposed Color Pass scheme, the user response time is expected to improve with each session as the orientation of the Feature Tables are fixed. So with each session user gradually gets familiar with the system and thus reply time also improve. This makes side channel attack quite challenging for the Color Pass system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

matching 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

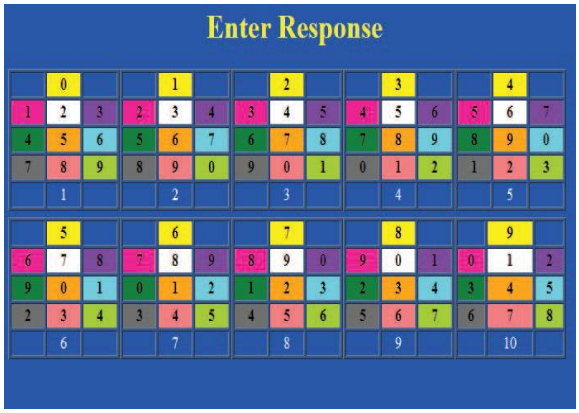

Fig. 2: User Interface On Screen

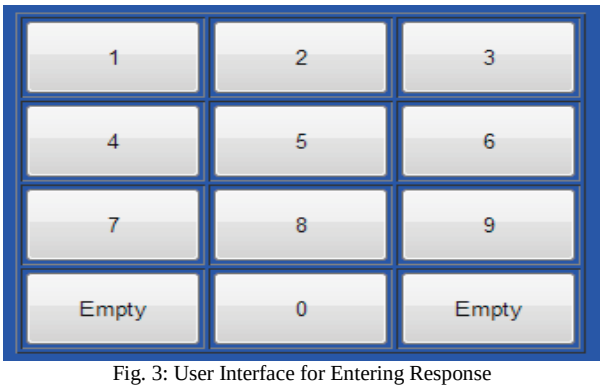

Fig. 3: User Interface for Entering Response

3.2 Usability Evaluation

System implement for use in public domain requires user sociability along with mechanism to protect sensitive details of the users. In our proposed method, we have found it efficient against attack like Shoulder Surfing or guessing the password. Our evaluation of usability and criticism from users also appear acceptable. We have perform our trial using the succeeding work station with configuration 4 GB

RAM, i3 core processor and processing speed of 2.40 GHz. We take help of 20 users to perform our experiment. First we give a broad overview about how the method works. The standard time taken by users to be aware of our means is about 10 minutes (mins). And the criticism we got from most of the users is that − our style is very easy to understand. It be theoretical to be well-known that we only give the users lecture about how to use the system. Our lesson does not comprise safety psychiatry of our outlook system. Each lesson age is about 5 mins. We chose the users from the student (12 students) and other people from the civilization (8 people).

IV. CONCLUSION

In this paper we have future a novel scheme to legalize a user using color PINS. The plan is identified as Color Pass scheme which provides an clever boundary 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 scaffold of incompletely apparent aggressor model. From

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

sanctuary point of view the scheme is quite strong against some promising attacks such as carry surfing, guess password, side channel attack, etc. And from usability point of view the scheme is user sociable and takes very less time for login. Also the tender can be used by both math and non-math sloping people. The planned slant shows trivial low error rate in login system. In occasion we will explore how to widen this scheme for fully obvious enemy 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. 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. Proceeding of the 2014 IEEE Students' Technology Symposium TS14HMI01