ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2015**

# A Survey on Color Password Authentication to Avoid Shoulder Surfing Attack

Priyanka S. Dahitule[1], Priyanka D. Borhade[2], Priyanka R. Wajage[3]

B.E. Students, Dept. of Computer Engineering, Jaihind College of Engineering, Pune, India

**ABSTRACT**: In shoulder surfing attack, an unauthorized user can fully or partially observe the login session .To avoid this attack we propose an intelligent user interface, known as Color Pass .This proposed system based on partially observable attacker model, i.e. the attacker can partially observe the login procedure. Classical PIN entry is a popular scheme because it greatly balances the usability as well as security aspects of a system .Color Pass interface is easy and safe for any genuine user. Authorized user can enter the session PIN without disclosing the actual PIN.

**KEYWORDS:** Shoulder Surfing Attack, Color Pass, Classical PIN, Partially Observe, Lookup Table.

## I.INTRODUCTION

The shoulder surfing attack in an attack that can be processed by the opponent to obtain the user's password by watching over the user's shoulder as he enters his password .As now a day there are a huge Internet users in the world. Our proposed software applications deal with sensitive as well as private information which must be saved from misuse by some malicious or unauthorized users and their attacks. Every security area, role of authentication is a very important technique by which the system can identify the type of users. There are many authentication schemes available among which password based authentication is most used as it is cost effective and secure. The shoulder surfing attack in an attack that can be performed by the opponent to obtain the user's password by watching over the user's shoulder as he enters his password .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 .In this proposed system it also provides equal number of password strength as classical PIN entry .Refer Fig 1.as given below.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2015**

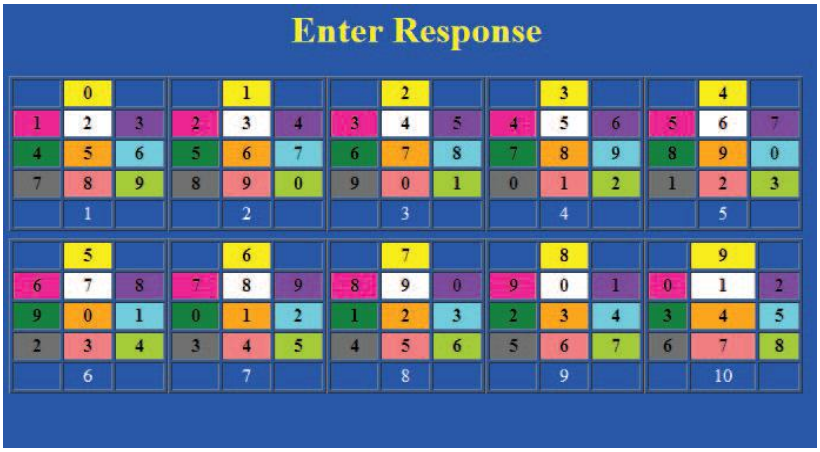


Fig 1 .Generate Feature Table

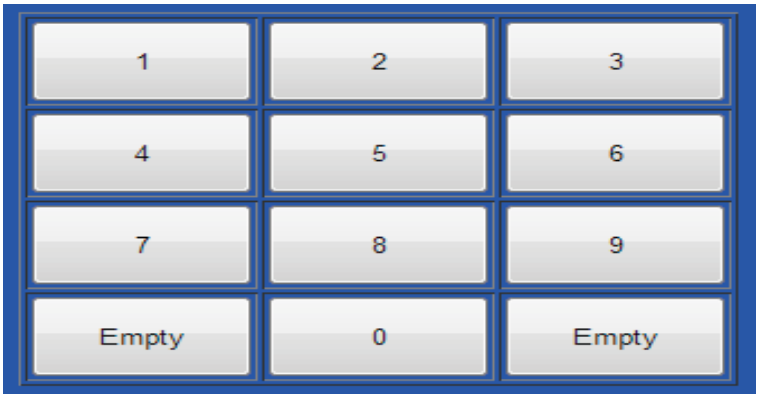


Fig 2 .Response Table

## II.RELATED WORKS

To login the system, user first enter his own login-id and the user has to enter password in a correct manner, pass the fore determined number of challenges. Our system is based on partially observable schemes which have motivated us to propose the Color Pass scheme for avoiding shoulder surfing attack.

## III.PROPOSED SYSTEM

In this section, we will describe a easy and efficient shoulder surfing resistant password scheme based on color Pass. The existing scheme involves 2 phases, the registration phase and the login phase .In past we studied many graphics GUI techniques to avoid shoulder surfing attack .In our proposed system it is based on partially observable attacker model. Thus it is assumed that the media through which user gets the challenge should ensure security against man-in-middle attack. In this paper, we will propose an improved color pass shoulder surfing resistant password scheme by using colors. The operation of the proposed scheme is simple and easy to learn for users familiar with color passwords.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2015**


Fig 3.Architecture of Color Pass Scheme

A .Characteristics of chosen PIN

In literature, users have to remember the some digits or characters with some special symbols as a password. But in our proposed scheme, colors are used for generating a new login PIN .Hence name as Color Pass Scheme.

B .Characteristics of feature table

Color Pass scheme consists of 10 different Feature Tables which are numbered from 0 to 10. Each cell of a table is represented by a pair < Ci, Vi >. Here Ci denotes the color of the cell i and Vi indicates the digit respected to cell i. Ci is unique with respect to a Feature Table. Thus, no color acquire in more than 1 cell. So for a particular table there will be 10 different color cells. The particular positions of color cells are shown in Table I and this is fixed for every table. So if first cell of a table is filled with C1 then first cell of all other tables are also filled with C1.

| | | |
|---|---|---|
| | 0 | |
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | K | |

Table I: Identifying Each Cells in K table

## IV.CONCLUSION

In this paper, we have proposed a simple text-based shoulder surfing resistant graphical password, in which the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the scheme without using any physical keyboard or on-screen keyboard. Finally, we have analysed the resistances of the proposed scheme to shoulder surfing and accidental login.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 10, October 2015**

## REFERENCES

[1] A. Paivio, "Mind and its evaluation: A dual coding theoretical approach," 2008.
[2] www.webeopdia.com/term/s/shoulder−surfing.html(last access october, 2013).
[3] "searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last access October, 2014)."
[4] 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, 2013.
[5] T. Perkovic, M. Cagali, and N. Rakic, "SSSL: Shoulder surfing safe login," in Software Telecommunications and Computer Networks, pp. 270– 275, 2012.
[6] "searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last 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 1996.
[8] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1999.
[9] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in ACM Conference on Computer and Communications Security, pp. 373–382, 2005.