Color Lock: Against Password Attacks

Priyanka D.Jagtap[1], Anjali K.Nathe[2], Ashwini H.Patil[3], Sayali R.Walzade[4],Prof.M. T. Jagtap[5]

[1] *BE, Computer Engineering, PVGCOEN, Nasik, India*
[2] *BE, Computer Engineering, PVGCOEN, Nasik, India*
[3] *BE, Computer Engineering, PVGCOEN, Nasik, India*
[4] *BE, Computer Engineering, PVGCOEN, Nasik, India*

ABSTRACT

The system identifies the genuine users ,in computer security, authentication is such a technique .Password based authentication is still one of the widely accepted ,among several authentication schemes .In which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN ,Color password is widely famous, but it is prone to shoulder surfing attacks .To a wide class of observation attacks such as brute force attacks, side channel attacks etc ,and traditional PIN-entry methods are vulnerable .Based on human cognitive skills have been proposed till date ,a number of alternative PIN-entry methods .These methods can be classified into two classes regarding information available to a passive adversary: fully observable and partially observable. So that any genuine user can enter the session PIN without disclosing the actual PIN ,In this system propose an intelligent user interface, known as Color Lock to resist the password attacks .On a partially observable attacker model ,the Color Lock is based .The experimental analysis shows that the Color Lock interface is safe and easy to use.

Keyword: - *Color PIN, Shoulder Surfing Attack, User Interface, Partially Observable.*

1. INTRODUCTION

In the world today, there is huge internet user's .Reported as approximately 2.4 billion worldwide, and from 2000 to 2012, it is a staggering 566.4% increase, in a recent report, the number of Internet users .These users can be both genuine and malicious users as well. To know which user is genuine or malicious ,nowadays it is very important .Which must be saved from misuse by some malicious or unauthorized users and their attacks ,Proposed software applications deal with sensitive as this system as private information .A very important technique by which the system can identify the type of users ,every security area, role of authentication. The most used as it is cost effective and secure ,there are many authentication schemes available among which password based authentication .To obtain the user's password by watching over the user's shoulder as he enters his password ,the shoulder surfing attack in an attack that can be performed by the opponent .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, the classical PIN entry mechanism is widely used because of its ease of usability and security.

Secure login methods can be classified into two broad categories completely observable and partially observable ,based on the information available to the attacker .The attacker can partially watch the login procedure ,In the first one, the attacker can completely observe the whole login procedure for a particular session and use it to gain knowledge about the actual pin and in the second one .To remember four color pins ,proposed system is partially observable and users have .This system use session pin without disclosing actual pin ,in the proposed methodology .The user sets four color as their pin ,in the proposed system. Corresponding to each color, User has to answer four challenge questions. The user has to remember four colors instead of remembering long alpha-numeric passwords. Also they are prone to brute force and shoulder surfing attacks, it is difficult for the users to remember long alpha-numeric passwords or graphical passwords. To conventional pin entry mechanisms, at the same time, Color Lock provides equal password strength compared.

2. LITERATURE SURVEY

In shoulder surfing attack, an unauthorized user can fully or partially observe the login session .To avoid this attack this system 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 this 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. 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 system, this system 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.

3. WORKING OF PROPOSED SYSTEM

- User enters his login id.
- Once system checks that the login id exists then it will generate Feature Tables using Algorithm 1.
- 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).
- User response will be evaluated by system using Algorithm 2.
- Finally system will decide whether the user is legitimate or not using Algorithm 3.

Fig 1: Table Generation

4. ALGORITHMS

4.1 Algorithm 1

Input: This algorithm will take array color [0,1,….9]as input

Output: It will generate Feature Table 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) mod10;
        end for
end for
```

Fig 2.Algorithm for generating table

4.2 Algorithm 2

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

Output: This algorithm will update value of array EVAL

by 1 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
```

Fig 3.Evaluating User Response

4.3 Algorithm 3

Input: This algorithm will take array EVAL as input after executing Algorithm 2.

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
```

Fig 4.User Authentication

5. SYSTEM ARCHITECTURE

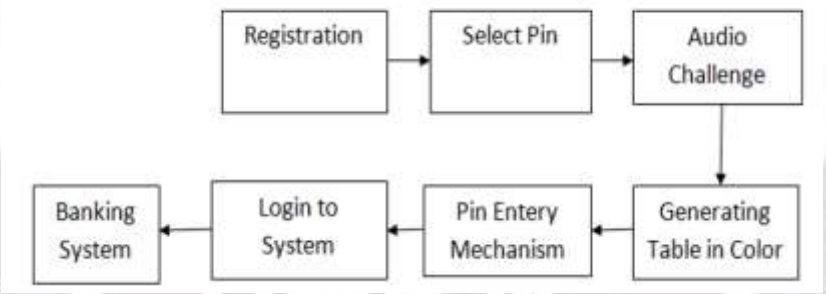

Fig 5: Architecture Diagram

In this system, First user have to do registration, then the audio value is generated and 10 tables are generated .Then pin entry mechanism is applied if resulting entered value is correct then user able to login to system.

6. CONCLUSION

In this proposed system a novel scheme to authenticate a user using color PINS. The scheme is known as Color lock 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 this system will explore how to extend this scheme for fully observable attacker model.

7. REFERENCES

[1] M.M.Group,"http://www.internetworld stats.com/stats.htm," June 2012.
[2] 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.
[3] T. Perkovic, M. Cagali, and N. Rakic, "SSSL: Shoulder surfing safe login," in Software Telecommunications and Computer Networks, pp. 270–275, 2009. [4]"searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last access october, 2013)."
[5] Colorpass: an intelligent user interface to resist shoulder surfing attacks.
[6] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM Journal on Computing, vol. 15, pp. 364–383, may 1986.
[7] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1996.
[8] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in ACM Conference on Computer and Communications Security, pp.373–382, 2005.