Special Issue - 2017

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICCCS - 2017 Conference Proceedings

Authentication using a Combination of Color Scheme and Musical Notes

Vimal Gaur[1]
GGSIPU,
Maharaja Surajmal Institute of Technology
Delhi, India

Akansha Singh[2], Ankur Chaturvedi[3]
GGSIPU,
Maharaja Surajmal Institute of Technology
Delhi, India

Shivam Dabral[4], Hiteshi[5]
GGSIPU,
Maharaja Surajmal Institute of Technology
Delhi, India

Abstract:- Security has become a major issue in existing world. There exist many methods to secure confidential information and passwords. But most of them as textual password, graphical password etc., are susceptible to shoulder surfing, brute force and dictionary surfing. These passwords can be easily predicted by attackers. There are other techniques also which rectify these attcks. One is color scheme and other is musical authentication. Both the schemes themselves are very strong and secured. Color scheme is an authentication scheme against shoulder surfing. The main aim of this project "Authentication using a combination of color scheme and musical notes" is to make the system complex for attackers. It also provide protection against shoulder surfing, brute force and dictionary attacks. This project uses a combination of both the schemes. This will provide color and musical notes based authentication to the user. This scheme authenticates the user by using session password. This authentication system makes data more secure and free from attacks. Here, the user only needs to remember the color rating done at registration phase. The whole process will only be based on this rating. Musical authentication is based on the principle that the music, melody can all aid memory. Musical passwords are easy to remember and are more secure since with each note there is a unique associated secret code. This combination of two schemes is highly memorable as for a particular music note, a specific color will be associated that defines for a session and defiant to brute force, dictionary attack and shoulder surfing attack. User can use different combinations of color and musical tune for creating password which will be complex for attacker to know the password. Speed and cost make this more efficient and can be used to encrypt large amount of data.

Keywords- Color scheme, musical authentication,

I.   INTRODUCTION

In today's era, computer society has been playing a major role in our lives and among that world security has always been a major issue. The more we indulge in technological applications, the more it deals with our personal information. This computer world does not comprise only professionals but also include hackers that are always in position to attack their prey. They stole our personal information through various attacks like shoulder surfing, brute force attack and dictionary attack etc. Hence, arises the importance of authentication. User authentication is a means of authenticating, or verifying, the identity of an individual requesting access to certain information.

It is an important security measure for protecting confidential information. Many authentication schemes has been proposed against such attacks. The most common method used for authentication [1] is textual password. The vulnerabilities of this method are well known. Arbitrary and lengthy passwords can make the system secure. But main problem with this was difficulty of remembering these passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily broken or guessed. The alternative techniques are graphical passwords and biometrics. Biometrics have been introduced but not widely adopted. Most of the systems are expensive and slow. Most of the graphical schemes also suffered from shoulder surfing which is becoming quite a big problem. A solution to this problem is a color authentication scheme [2]. This scheme is very different from other schemes and uses color as password. It's quite interesting. Another good authentication scheme proposed is musical authentication [3]. This scheme was based on the principle that the music, melody can all aid memory.

In our proposed scheme, a combination of two schemes has been used that is color authentication scheme and musical authentication. In this scheme, the user needs to rate the colors and on the basis of that rating, a number will be generated that will be known only to the user. The number that we have obtained from the grid will be used in further authentication. Only those piano keys will be pressed that will correspond to the number obtained. A tune will be played on pressing the keys and the code associated with each key will be inputted as password. This scheme will rectify all above mentioned attacks.

II.   LITERATURE SURVEY

In 2002, to reduce the shoulder surfing attack, Sobrado and Birget [4] proposed three shoulder surfing resistant

Special Issue - 2017

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICCCS - 2017 Conference Proceedings

graphical password schemes, the Movable Frame scheme, the Intersection scheme and the Triangle scheme. The first two schemes fail frequently in the process of authentication.

In 2006, to overcome the drawbacks of Sobrado and Birget Scheme, the Convex Hull Click Scheme is proposed by Wiedenbeck et al. [5]. It is an improved version of the triangle scheme with great security and usability.

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. [6]. This scheme has drawbacks like, the probability of accidental login of Color login is too high and the password space is too small.

In 2012, a new authentication scheme has been proposed [3], based on the principle that the music, melody can all aid memory. In this scheme, the simulation of Piano instrument is implemented for proof of concept. User creates the music using the keys of Piano simulation, which will be stored as user password in the secure database. Each key selection of piano can be associated with a unique secret code, the combination of these codes are actually stored in the database after hashing, which will be tested at the time of user authentication. The proposed scheme is highly memorable, defiant to brute force attacks and dictionary attack, protected from shoulder surfing attacks and from spywares tracking.

In 2015, to overcome drawbacks of various authentication schemes and to shoulder surfing, color authentication scheme has been proposed. This is session password scheme in which the passwords are used only once for each session and when session is completed the password is no longer in use. This scheme uses colors and text for generating session password.

III. PROPOSED SCHEME

In this paper, a new scheme has been proposed that uses a combination of both color scheme and musical scheme. Both the schemes are themselves very strong and secured hence a combination of both schemes will be a great challenge for attackers.

Main aim of this scheme is to create a password that is going to use color and musical notes as password instead of direct text or numbers. In this scheme, a registration and login process has been shown. In the first part, color scheme has been implemented and then using the rating of first part, musical scheme has been implemented.

This project has been divided into two parts-registration phase and login phase.

Registration phase

First, we have to register ourselves during the signup phase. In this we need to enter our username and email

besides some other basic credentials. Then we have to rate the colors in any way that we want to. This color rating must be remembered by the user to login at the time of login.
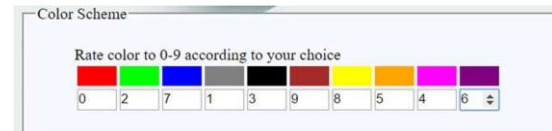

Fig1- details of the user

Fig2- colour rating

The user can give the rating to the colors as per their choice. They can also give same color rating to more than one color. The only requirement is that they have to know the rating of each colour at the time of login. The figure shows how to give the rating to each colour.

After user submits the form, the details and the colour ratings are saved in the database.

```
$conn = new mysqli("localhost","root","","ankurdb");

if($conn->connect_error)

{ die('Error in connecting with database'. $conn->connect_error); }
```

After successful connection to the database we insert the data that is retrieved from the form into the registration table.

```
>$uname = mysqli_real_escape_string($conn, $_POST['uname']);
```

Login phase
During login phase, user needs to enter his username and email-id and have to click the button. When he clicks the button, a random sequence of colors is generated for him. There is a 2- dimensional square matrix of order 10 provided to the user. Using this matrix with the help of sequence generated the, user needs to enter the password.
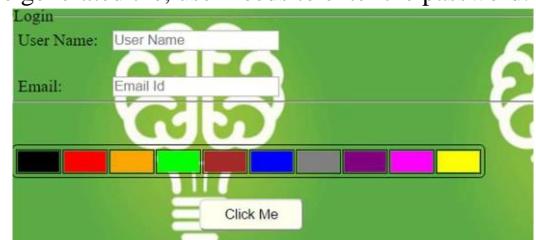

Fig3- randomly generated colour sequence

Clicking the button, you can generate the sequence and clicking it again will change the sequence if the user wishes to do it.

Fig4-   the   matrix

using the color sequence of color and the rating that the user had given during the registration phase, the user makes group of two from the sequence where the rating of the first color represents the row and second color represents the column of the matrix.

After that user needs to check the corresponding number in the matrix that is the intersection element of the row and the column that is determined by the sequence of the color.

```
function genseq(min, max){

        min = Math.ceil(min);

        max = Math.floor(max);

        var x = Math.floor(Math.random() * (max - min)) +
min;

        seq(x);
```

This function generates a random number between the two numbers that are fed as the arguments and then calls another function seq() with an integer argument that has been randomly generated by the random() function.

This seq() function will now generate the random sequence of colors that is displayed on the webpage.

After checking the sequence of colors and the matrix to get the password, user have to play the piano provided to him to enter the password and no other means of input can be used for entering the password.

The piano made is just a part of the full 88 keys piano just to demonstrate the use of it. Every key has a number associated with it which also changes randomly whenever we click the button. The numbers are used to for the users those who don't have any knowledge of musical notes. It makes it easy for the user to recognise the piano key that is needed to be pressed for entering the correct password. The concept to generate the random sequence of numbers is same as that of generating the colour sequence.
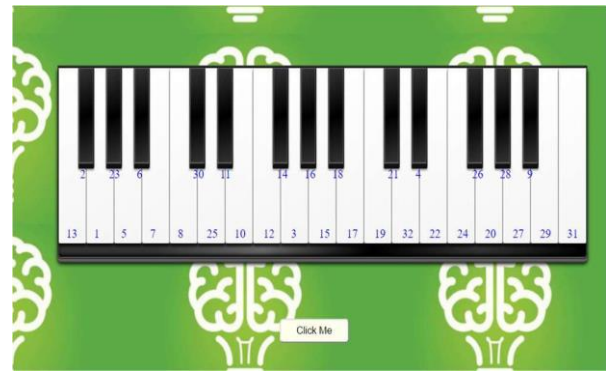

Fig5 - piano with random numbers on keys

After having the number obtained from the matrix, user will press only those keys that corresponds to the number obtained from the matrix. The keys are numbered randomly and this sequence changes every time the user login to the system.

For every key there is a secret code associated to it that is stored in the database and is appended to the password textbox every time we press a key of the piano.

Fig6 – the code being appended in the password box

The secret code made it difficult to apply a brute force attack to retrieve the password.

Fig7 – the code associated to keys and saved inside database

Each key of the piano has separate id associated to it which is used to get to know which key is being played.

```
$(document).ready(function(){ var c =
  $("#mid-c")[0];
```

```
var cs = $("#mid-c-sharp")[0]; var d =
$("#mid-d")[0];
var ds = $("#mid-d-sharp")[0]; var e =
$("#mid-e")[0];
var f = $("#mid-f")[0];

var fs = $("#mid-f-sharp")[0]; var g =
$("#mid-g")[0];
var gs = $("#mid-g-sharp")[0]; var a =
$("#mid-a")[0];
var as = $("#mid-a-sharp")[0]; var b =
$("#mid-b")[0];
```

Using these variables, make it easy to recognise which key is pressed, and the corresponding frequency of sound is produced every time that key is pressed.

As the keys are pressed and the form is submitted, the string from the password is checked and the password retrieved from it saved.

A similar procedure runs in backend to calculate the password using the original colour rating that was entered by the user at the time of registration. The password is generated from the sequence of colour and the matrix in a similar.

Now this password that is calculated is compared with the once entered by the user using the login phase. If the password matches the user is given access to site otherwise not. Comparing the colour rating with the database rating entered by the user using the logic given below-

```
for ($p = 0; $p <= 9; $p++){     //for checking the

$myArray values

    if (!(strcasecmp($myArray[$p],'red'))){$intseq[$p] =
$row[2]; }

    else if(!(strcasecmp($myArray[$p],'green'))){$intseq[$
p] = $row[3]; }

    else if(!(strcasecmp($myArray[$p]
,'blue'))){$intseq[$p] = $row[4]; }
```

Assigning the numbers from the matrix and array for further comparison

```
for($i=0; $i<5; $i++){ if($ans[$i] ==
    $dbpass[$i]) continue;

    else break;
  }
```

Comparing the two passwords and redirecting to the appropriate page

```
  if($i==5){
```

```
    header("Location: welcome.php? user= $uname");

  }

else{

  echo "password incorrect";
  header("Location: invalid.html");
  } }
```

IV.   PROTECTION

This scheme provides protection at four stages:

1. The color rating is done at registration phase. So, only the user know about the rating that he has done.
2. After login, depending on the rating, a number will be generated form the grid. Since the grid contains randomly distributed number and also the rating is not known to the attacker, the attacker will never came to know the number generated.
3. Only those keys will be pressed that corresponds to the number generated. On every login, this numbering will going to be change.
4. The code associated with the keys pressed will be inputted as the password and that too will be in a hidden form.

At each step shoulder surfing is prevented along with other attacks.

V.   RESULT ANALYSIS

After completing the whole process, the code is successfully inputted into the password. The first aim of this scheme is to generate a number from the grid with the help of color rating. This process has been completed successfully. The rating done here is unknown to the user. During the whole procedure, the user has to remember only this rating. It is not as much complicated as others. It completely depend upon user, what type of rating he wants to give. It could be different numbers or same numbers. After pressing the submit button, the user can login to the system.
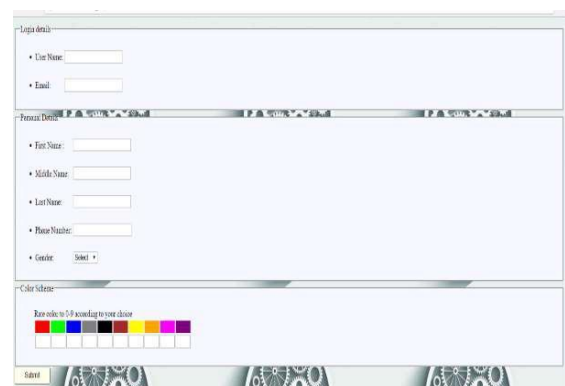

Fig.8 registration page

Special Issue - 2017

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
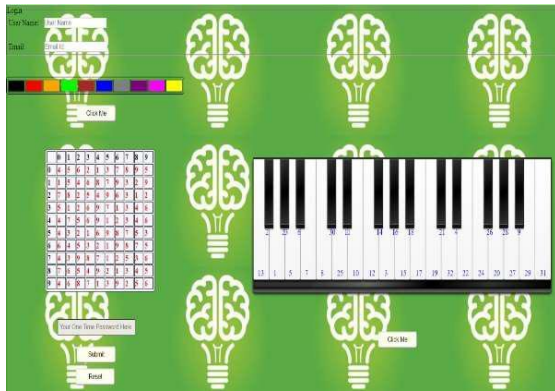**ICCCS - 2017 Conference Proceedings**

Fig.9 login page

The second aim of this scheme is to play the piano and the code associated with the keys should be inputted as password. This has been achieved successfully. This scheme is really very helpful in organizations as it is very flexible, attractive, much secured, and overcomes shoulder surfing, brute force and dictionary attack.

VI. CONCLUSION

Many authentication schemes has been proposed for shoulder surfing type attacks like graphical password etc. Every scheme has an disadvantage. To overcome these attacks, two schemes has been proposed that is color and musical schemes. This proposed scheme uses a combination of both schemes which results out to be a very good scheme and as a great challenge for attackers. The user has to remember only the rating, no need to learn long passwords. Also, the user does not need to press any key which prevents from shoulder surfing. By chance, if the attacker watch the user while pressing the keys then, when attacker try to login, the numbering of keys will be changed randomly. Hence, this scheme is really good.

REFERENCES

[1] G.E.Blonder, "Graphical Password", in Lucent Technologies, Inc., Murray Hill, NJ, U.S. Patent, Ed. United States, 1996

[2] Shefali Amlani, Shweta Jaiswal and Suchitra Patil, "Session Authentication using Color scheme" in proc International Journal of Computer Science and Information Technology (IJCSIT),2015

[3] Naveen Kumar," User Authentication using Musical password", in proc Interbnational Journal of Computer Applications, Decembar 2012

[4] L. Sobrado "Graphical passwords," The Rutgers Scholar," An Electronic Bulletin for Undergraduate Research, vol. 4,2002

[5] S. Wiedenbeck and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," Proc. Of Working Conf. on Advanced Visual Interfaces,May. 2006, pp. 177-184.

[6] H. Gao, X. Liu and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on\ Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.

[7] Jean-Camille Birget, Dawei Hong and Nasir Memon, " Graphical Password based on Robust discretization", IEEE transactions on Information Forensics and Security, Vol.1, No. 3, September 20006

[8] Sadie, Stanley E. , " The New Grove Dictionary of Music and Musicians", 1996

[9] Sandip Dutta, Chandan Kumar and Soubhik Chakraborty, " A Symmetric key algorithm for cryptography using music", in proc International Journal of Engineering and Technology (IJET)