TCM: Password Protection Using Text And Color Matrix

Shruti Bhavsar¹, Tejasvini Waingankar², Rupali Thorat³

¹B.E Computer, Pune University, JSPM’s BSIOTR(w)
Pune, Maharashtra, India
shrutib56@gmail.com

²B.E Computer, Pune University, BSIOTR(w)
Pune, Maharashtra, India
tejsvinw111@gmail.com

³B.E Computer, Pune University, BSIOTR(w)
Pune, Maharashtra, India
ripsthorat@gmail.com

Abstract

In today’s world, there are many techniques for protecting the passwords. These techniques are vulnerable to different attacks such as shoulder surfing, eaves dropping, dictionary attack, spyware etc. Graphical passwords have their own disadvantages. Complicated passwords are difficult to remember. For this, we have come up with new technique which is coupled with two new techniques. We are using text password and color password for which session passwords are created for both. For every login user input is different password. The password is generated using text and color rating which are resistant to various attacks. It can be used where security is of main purpose such as net banking, trade transactions, server-side etc.

1. Introduction

There are different techniques used for authentication such as textual password, graphical password etc. However they have their own disadvantages. Random and lengthy passwords difficult to remember. In this paper, we proposed a two level authentication scheme which provide higher security than existing system. Password is generated using text password and color rating. This passwords can be used only at that particular instant.

As soon as the session expires, the password is no longer valid. As such the user, keys in distinct passwords each time he logs into the session. The proposed system provides higher security against various attacks.

The proposed system using new authentication technique consists of two different techniques—textual authentication scheme and color textual authentication scheme.

2. Related Work

Syukri [1] developed a technique, in this password is a user’s signature. User draw signature using mouse. It is a complicated process. Drawing with mouse in the same perimeters which registered is difficult task.

Zhao and Li [3] proposed a shoulder-surfing resistant scheme “S3PAS”. In this make different combinations of password. Select approximate middle symbol of invisible triangle as a password. It provides higher security. But selection of middle symbol in large triangle is difficult.

Jermyn, et al. [4] introduced a technique called “Draw a Secret”. In this password technique user draw a picture as a password which is similar to registered password. For authentication picture draw on same grids in same order. It is vulnerable shoulder surfing. Drawing password is very difficult task.
Dhamija and Perrig proposed a graphical authentication in this system, where the user selects a number of images as a password. While authentication, the user has to identify the predefined images for authentication. In this, the number of images is difficult to remember, and the password is vulnerable to shoulder surfing.

Passface is a technique where there are nine human faces in a grid. The user selects four human faces as a password. While login, the user has to identify those faces to prove user's authenticity.

Man, et al proposed a technique where the user selects pass objects. Each pass object has a unique code. While login, the user has to enter the unique code of predefined pass objects. The user has to remember the pass object's code.

3. Proposed Technique
In this paper, we propose a new authentication scheme using session passwords, color ratings, and text.

During the registration phase, the user enters a normal textual password and also specifies the ratings to the colors, which will be called color passwords. Thus, two passwords will be registered: textual and color. The main constraint is that the textual password should be at least 8 characters long. The color pattern remains the same, i.e., RGBY, and the user can rate this color pattern from 1 to 4.

At the time of login, the user has to login with the help of a session password generated. Finally, the entered password is verified during the verification phase.

3.1. Architecture
In this, first of all, at the time of login, the user will be shown the two matrices: one for the textual password and the other for the color password. The user has to enter the session password based on these two matrices. Initially, the user will be displayed with the textual matrix. Based on this, the session password will be generated and entered. Then the color pattern will be displayed, where the user has to create the rated password. Using this password, the session password will be created based on the color matrix. Then this session password is entered. Finally, both generated session passwords are checked at the server because the server is also creating the session password at the backend. If they match, the user is allowed to access the homepage or other pages.

The basic architecture of the proposed technique is as shown below in the following figure.

Hence, there are two schemes for generating the session password: Textual Authentication Scheme (TAS) and Color Authentication Scheme (CAS).

3.1.1. Textual Authentication Scheme
In this scheme, the session password is generated for the textual passwords. At the time of login, an interface grid of 6 x 6 matrix is displayed. This matrix is alphanumeric in nature, changing every time for each login. This scheme works in various steps. First of all, the registered password (secret pass) is divided into a pair of two characters. The first character represents the row element, while the second character represents the column element. Then the intersection of both these elements is the session password, which is alphanumeric in nature. This process is repeated for other pairs also, and similarly, the session password is generated. To understand this concept, let us take an example. Consider the secret pass as "IJCTA1". Then, first, break that password into pairs as "IJ CT A1". Then, as per discussion, the first character is the row element, and the second character is the column element.
and their intersection is the session password. Hence, I is row element and J is column element. So we will search for the intersection of this two elements in the following interface grid as follows:

<table>
<thead>
<tr>
<th>A</th>
<th>F</th>
<th>0</th>
<th>M</th>
<th>7</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>L</td>
<td>1</td>
<td>3</td>
<td>T</td>
<td>Z</td>
</tr>
<tr>
<td>1</td>
<td>W</td>
<td>R</td>
<td>9</td>
<td>D</td>
<td>5</td>
</tr>
<tr>
<td>S</td>
<td>C</td>
<td>U</td>
<td>J</td>
<td>O</td>
<td>E</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>G</td>
<td>4</td>
<td>N</td>
<td>8</td>
</tr>
<tr>
<td>K</td>
<td>Y</td>
<td>V</td>
<td>B</td>
<td>Q</td>
<td>X</td>
</tr>
</tbody>
</table>

“Figure 3. Intersection of I and J”

Thus, we will get 3 as intersection element which is nothing but the session password for IJ pair. Likewise we have to search for the next intersection elements for the other pair. So, by looking into above grid for next 2 pairs we get, O as session password for CT pair and A as session password for AI pair.

Thus combining the individual passwords of every pair, we get 3OA as a session password for secret pass “IJCTA1”

### 3.1.2 Color Authentication Scheme

In this scheme, the session password is generated for the color password. This scheme considers the ratings given to the color pattern at the time of registration phase. During login phase, once textual authentication is done then, the user has to do the color authentication.

At the time of color authentication, new color pattern is displayed. This pattern consists of randomly placed colors (not “RGBY”). Then the user has to set the range for newly pattern according to registered color password.

Let’s understand with the example. Consider the ratings given during registration phase is 4213 for “RGBY”. Then at the login time, if suppose following pattern is displayed then according to registered color password, the user will rate the color as follows:

From the above figure it shows that at the registration time the rating for yellow is 3, for red it is 4, for blue it is 1 and for green it is 2. So based on the registered ratings, we have set the ratings for this color pattern which is displayed during login time. This newly given rating is called as rated password. Thus in our example, 3412 is the rated password. This pattern changes for every login phase and thus the rating also changes for every login phase.

Now, the 4x4 matrix is displayed which consists of digits numbered from 1 to 4. This digits are also placed randomly such that no two elements are placed in one row and column and changes for every login session as shown below:

```
1 2 3 4
1 3 4 2 1
2 2 1 3 4
3 1 2 4 3
4 4 3 1 2
```

“Figure 5. Color matrix during login phase”

Once we have rated the colors, the next step is to divide the ratings into a pair of two such that first digit is row element and the second digit is the column element. The intersection of these two elements is the session password.

So, in our example, the rated password 3412 is broken into a pair of two as 34 and 12. Now, as per previous statements, 3 is the row element and 4 is the column element. Now, we will search for the intersection element for 3 and 4 in the above color matrix. After searching, we get 3 as intersection digit which is the session password for 34. Likewise, we will generate session password for the remaining pairs. Hence, for another pair i.e 12, we get 4 as session password. Thus, by combining, we get final session password as 34 for rated password “3412”.

Finally, both the session passwords i.e one obtained in textual authentication scheme and another in color authentication scheme are checked at the server side. If it corrects then the user is allowed to access the particular homepage or
4. Algorithms

To implement this paper, we have two algorithms for the proposed technique. These are:

1. Textual authentication scheme
2. Color authentication scheme

4.1 Textual Authentication Scheme

The algorithm for this scheme is as follows:

1. User should submit the password during registration.
2. Minimum length of the password is 8 and it is called as secret pass. The secret pass should contain even number of characters.
3. Generate a 6x6 grid consisting of all alphanumeric characters placed randomly in the grid.
4. Divide the secret password in pairs of two.
5. Calculate the no of pairs and store it in n.
6. Set i=0
7. While i is less than n do
   a. The first character of pair i represents the row number(x) and the second character represents the column number(y).
   b. The intersection character of x and y is the session password for the pair i.
8. Submit the final session password.

FORMULA

Let M be the 6 x 6 matrix.
Let n be the no of pairs in secret password.
Let x be the first character of the pair at i
Let y be the second character of the pair at j
Let Z be the session password.

\[ Z = \sum_{m=0}^{n} Z[m] = M[x][y] \]

4.2 Color Authentication Scheme

For this the algorithm is as follows:

1. User should submit the rating of four colors (Red, Green, Blue, Yellow) from 1 to 4 during registration.
2. Generate a 4 x 4 grid consisting of numbers placed randomly in the grid.
3. At the time of login, 2 pairs of colors will be generated randomly.
4. Set i=0
5. While i is less than 2 do
   a. The rating of the first color of pair i represents the row number(x) and the rating of the second color of the same pair represents the column number(y).
   b. The intersection number of x and y is the session password for the pair i.
6. Submit the final session password.

FORMULA:

Let M be the 4 x 4 matrix.
Let x be the row number of the i th pair
Let y be the column number of the i th pair
Let Z be the session password.

\[ Z = \sum_{m=0}^{n} Z[m] = M[x][y] \]
5. Implementation

To implement this paper, following two types of requirements have to be considered:
1. Functional
2. Non functional

5.1. Functional Requirements

These requirements include:

5.1.1. JDK 7

This is the Java Development Kit (version 7) software, which provides the developer as a project coin support. It also provides the editor enhancements (code completion, hints etc).

5.1.2. Eclipse

Eclipse is an open source community whose projects building tools and frameworks are used for creating general purpose application. The most popular usage of Eclipse is as a Java development environment. Eclipse is an open source community, whose projects are focused on building an open development platform comprised of extensible frameworks, tools and runtimes for building, deploying and managing software across the lifecycle.

The Eclipse Project was originally created by IBM in November 2001 and supported by a consortium of software vendors.

5.1.3. MySQL

The database that will be used for will be MySQL, as MySQL database are easily portable.

As the main motto of the project is providing session password for the user, we will need a table to store the session password of the user. This table will store both the secret password entered from the grid and the color password.

5.2. Nonfunctional Requirements

1. Secure access of confidential data (user’s details).
2. High Scalability. The solution should be able to accommodate high number of customers and brokers. Both may be geographically distributed.
3. Flexible service based architecture will be highly desirable for future extension.
4. Better component design to get better performance at peak time.

6. Analysis

There are many disadvantages of existing systems to overcome that we proposed a new technique authentication scheme TCAS.

1. Textual passwords, passface, graphical passwords are vulnerable to shoulder surfing. These technique is Shoulder Surfing Resistant. Because every login process, user input different password.
2. Password can be cracked by dictionary and brute force attacks. It provides better security against dictionary and brute force attacks.
3. In Graphical passwords, passface identification process can be slow. Some passwords are complex.
4. S3PAS technique provides higher security but finding approximate middle character in triangle complicated process. Proposed technique provides higher security by using easy process.

7. Conclusion

The authentication scheme is proposed for PDAs (Personnel Digital Assistants). These scheme authenticate the user by session passwords. For every login process, users has to enter different passwords. The session passwords provides higher security against various attacks such as dictionary attack, brute force attacks as password changes for every session.

However, this scheme is completely new to the user but if it practiced then user will find it easy to the process for generation of session password. Thus, it reduce the complexity and increase the usability.

8. Future Scope

In India, this authentication scheme is not used in any net banking application. So the banks can adopt this authentication scheme for improving their security.

Besides, this scheme can be used in:
1. Military
2. Companies to store their secret data.
3. Lockers
4. Any other application where security is the main concern.

References


