Color Shuffling Password Based Authentication

Aayush Dilipkumar Jain¹, Ramkrishna Khetan², Krishnakant Dubey³, Prof. Harshali Rambade⁴
Department of Information Technology
Vidyalankar Institute of Technology, Mumbai, India

Abstract:
Many password authentication schemes have been proposed. Many shoulder surfing resistant graphical password scheme has been proposed and most users are more familiar with textual password than graphical password but in that many security problem is created. So same year ago many text based graphical password scheme has been proposed but unfortunately none of exiting text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this proposed scheme, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.

Keywords: CCP: Color Click Points, SSO: Single Sign On, CPA: Color Password Authentication

I. INTRODUCTION

Various color password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling Colors than text. Color passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by Colors, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. In our project, we propose a new click-based color password scheme called Color Click Points (CCP). It can be viewed as a combination of Pass-Points, Pass faces, and Story. A password consists of one click-point per Color for a sequence of Colors. The next Color displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security. Users could quickly create and re-enter their passwords. Another feature of CCP is the immediate implicit feedback telling the correct user whether their latest click-point was correctly entered.

II. LITERATURES URVEY

Nowadays alphanumeric passwords are getting used for user authentication. Textual alphanumeric passwords were first introduced in the 1960s as a solution to security issues. While today possible alternatives are biometrics, Face recognition mechanism, Retina scan and smart cards, passwords are likely to remain in use for some time because it provides reliability, privacy, security, and ease of use of other technologies such as biometric, face recognition, retina scan needs hardware support. However, the use of passwords dilemmas often arises in the tradeoff between security and usability. Passwords should be easy to remember, and authentication protocol should be quickly and easily executable by humans. Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user. In an effort to improve password researchers have developed graphical passwords. However, the problem of shoulder surfing is a recognized drawback of graphical passwords. [1] Various color password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling Colors than text. Color passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by Colors, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. Users could quickly create and re-enter their passwords. Another feature of CCP is the immediate implicit feedback telling the correct user whether their latest click-point was correctly entered. Click Color points is a click-based color password scheme, a Color-recall color password technique. Users click on one point per Color for a sequence of Colors. The next Color is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to Pass Point, saying that selecting and remembering only one point per Color was easier, and that seeing each Color triggered their memory of where the corresponding point was located. CCP also provides greater security than Pass-Points because the number of Colors increases the workload for attackers. Passwords possess many useful properties as well as widespread legacy deployment; consequently we can expect their use for the foreseeable future. Unfortunately, today’s standard methods for password input are subject to a variety of attacks based on observation, from casual eavesdropping (shoulder surfing), to more exotic methods. Shoulder-surfing attack occurs when using direct observation techniques, such as looking over someone’s shoulder, to get passwords, PINs and other sensitive personal information. As well as when a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user’s password credentials. This is a problem that has been difficult to overcome. [3] The correctly entered password appears to be random and can only be derived with the knowledge of the full set of password objects. Therefore, it would be difficult for a shoulder-surfing adversary to identify the user's actual password. Simulation results indicate that the correct input object and its location are random for each challenge set, thus preventing frequency of
occurrence analysis attack. User study results show that the proposed method is able to prevent shoulder-surfing attack. [5]

III. PROPOSED SYSTEM

In existing systems it is very easy for attacker to decrypt users password, it only provides one level of security i.e. the password, and if the attacker knows the password there is no other security level that can prevent it from accessing the users data. In our Project, we make it easy for the user to login to the system. Also, to establish a secure transaction between the User and the Server. We will develop an application which will provide security against Shoulder Surfing Attack. This system will provide 2-Level security to the registered User. Our Project will provide Single Sign On (SSO) feature to our clients. This project will make attacks based on hotspot analysis more challenging. The incoming data to the product would be raw text data and Colors. The outgoing data would be the text and Colors. A database is maintained to store the text and information about the Colors.

IV. WORKING

1. Click-based color passwords: The category of click-based color passwords includes password schemes where users are presented with a Color (or series of Colors) and enter their password by clicking on specific areas of the Color.

2. Click-point: A click point is as a specific pixel within an Color that a user has clicked on with the mouse (or other pointing device).

3. Tolerance region: It is a small area on an Color which is used while click points password that provide us with approximation or tolerance area within which click point is considered as valid.

4. Color Password Authentication (CPA): Color Password Authentication is a way of providing authentication to users that works by having user select from Colors in a specific order presented in Color User Interface.

5. Color Recall technique: It is a color password technique which is extension of recall based technique where an extra cue in provided to users to remember and target specific locations within presented Color.

6. Color Click Point (CCP): It is a Color-recall color password technique in which users click on one point per Color for a sequence of Colors where the next Color is based on previous click-point.[3]

Intended Audience

This document is intended for both the users and the developers of the system. Our software’s intended audience are the higher authorities of organizations. For example: Bank Managers

V. METHODOLOGY

In this project we are using java as our basic coding language. We are implementing our java code using java visual studio. The reason behind using java as our basic coding language is that, it is easy to learn and implement, it is open source software and also it is very simple to implement it on other platforms as it follows the principle of write once and run anywhere.

A. Algorithm for Color Wheel Generation:

1. Read the line end points(x1,y1) and (x2,y2) such that they are not equal. If they equal then plot that point and exit.

2. dx=|x2-x1| and dy=|y2-y1|

3. [Initialize starting point] x=x1 , y=y1

4. e=2*dy-dx

5. i=1[Initialize counter]

6. Plot( x , y)

7. while(e>=0)

   { y=y+1 e=e-2*dx } x=x+1 e=e+2*dy

8. i=i+1

9. if(i<=dx) then go to step 6

10. Stop

B. Algorithm for Random Number Generation:

Input: 10 character, 0 to 9=10

Output: Random Printing Algorithm:

1. To generate the matrix wit row and column 8*8.

2. Put 0 to 9 numbers into matrix.

3. Select one random number from 0 to 9.

4. For putting number into matrix system check number is already present or not.

5. If number present then perform Step3. If not present then put into a matrix and go to step3.

6. Do step 5 repeatedly upto 0 to 9 inserted into matrix.

7. Print The Matrix.

8. Repeat Step 3 to 7 for each matrix.

9. Now Get string which have 10 character, “0 to 9=10” .

10. Get number present into matrix sequentially [0] [0] to [10] [10] i.e., total 100 character .

11. Select index of string from 100 char. put into that current location .


13. Print Current Matrix.


15. Stop

VI. ANALYSIS

System Analysis is the detailed study of the various operations performed by the system and their relationships within and outside the system. Analysis is the process of breaking something into its parts so that the whole may be understood. System analysis is concerned with becoming aware of the problem, identifying the relevant and most decisional variables, analyzing and synthesizing the various factors and determining an optimal or at least a satisfactory solution. During this a problem is identified, alternate system solutions are studied and recommendations are made about committing the resources used to design the system.

VII. CONCLUSION

In this paper of color shuffling we prevent shoulder surfing attack up to some extent which on future implementation can lead to minimum shoulder surfing. In this system user can easily login into system without worrying about shoulder surfing and key logger attack. User just have to remember color of sector and numeric password. This scheme is simple and efficient. Unlike other graphical password scheme user can easily log into the system without remembering graphical sequences. This system does not need use of physical or on-screen keyboard.

VIII. REFERENCES


[5]. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev. in press.
