

Color Code Based Authentication And Encryption

Rajesh N¹, Sushmashree S², Varshini V³, Bhavani N B⁴, Pradeep D⁵

Student, Information Science, National Institute of Engineering, Mysore, India^{1,2,3,4,5}

Abstract: In today's high technology environment, organizations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing. Today's information system the security is largely supported by password for authentication process. The most of password contains alphanumeric and special characters it is highly vulnerable. To overcome the drawbacks of traditional method we propose new authentication method to abolish well known Security threats like brute force, dictionary attacks phishing attacks and spyware attacks. Encryption is a process of changing the data into unreadable format, much of the data flows through information system is highly sensitive need to be protected, and the disadvantage of widely used public key encryption is time consuming. Public-key encryption may be vulnerable to impersonation, even if the intruder not able to get private key. A massive attack on a highly secured network will allow an intruder to imitate or mimic the adversary chooses to by using a public-key from the compromised security network to the key of the adversary's choice in the name of another user. To overcome the drawbacks of traditional encryption we introduce RGB color code oriented encryption method. The data consists of characters, symbols and digits. The data are converted in ASCII value, then these ASCII value are grouped into four digits and then the each part is assigned typical html RGB color codes, then these codes are converted into binary values and the binary values are compressed using simple XOR operations. Finally the data transmitted to receiver

Keywords: Include at least 4 keywords or phrases.

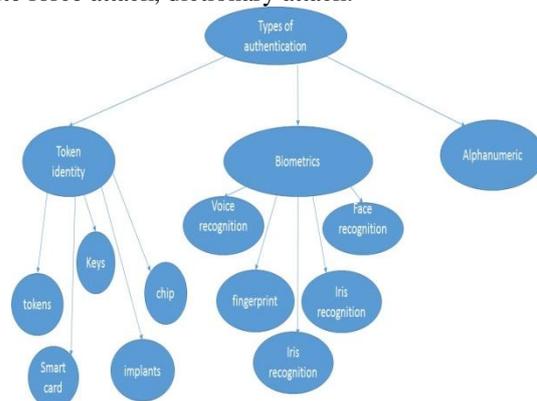
I. INTRODUCTION

Authentication verifies the identity of an Account Holder. Authentication is important for providing Security of the System. Authentication is done by String of alphanumeric and Special Characters that allows access to the computer, interface... etc. and also called password. Password is the Key to authenticate user account. Text key (password) is the most common method for authentication. The general method is more vulnerable to various cyber-attacks like phishing, spyware attacks, dictionary attacks, brute force attack etc.

To overcome the problems faced by general method alternative authentication models like biometrics used. But the biometric authentication is for Top level security and this authentication system involves a lot of expense. Now a days there more talked about graphical password in the industries.

Now a day's banks and financial institution using one time password and it was also called as OTP. Besides OTP offers better security. it is impossible for hacker to break into the OTP Using conventional attack. But the OTP was very expensive it is not for general purpose user, we introducing new kind password matrix which solves most of the problems like phishing, spyware attacks, dictionary attacks, brute force attack. The color code matrix password was only used for the only one time like OTP because it changes for every refresh of the page. The color code matrix password is virtual password it was created by system for that instinct.

The color code matrix password contains alphabets and numeric values which was represented in six rows and six columns. It was arranged in 6*6 matrix or grid. The each row [0] and column [0] contains the color background. The color includes anyone in the set, the colors in the set are red, yellow, green blue, white, and pink. The background color was chosen randomly. The background color varies for each refresh. With the use of color code matrix you can openly type your password the people around you cannot know your password, the color code password matrix cannot be detected or guessed by any software, the color code matrix overcomes the fear of brute force attack, dictionary attack.



The existing picture passwords are very complicated and time consuming for the Authentication. An Authentication system require more computing power for pictured

passwords while affecting the performance. We present this approach to propose a Color code matrix authentication password scheme.

The concept of using rgb color code encryption is an innovative idea, The RGB color model is combinational of three different types of color. The combinations of red, green and blue light provides huge combination and wider variety of color spectrum. The general uses of the RGB color model is to project the images in electronic systems, like movies and photos in television screens and computer monitors and it's also used in high definition photography. CRT, LCD, plasma and LED TV and monitors all uses the RGB model. We are using the same technique in our project, the each key in the keyboard contains the ASCII key, the combination of ascii key and present time provides us 8 bit to 24 bit RGB color representation, these 8 to 24 bit representation gives access to 16 million different colors.

II. PROPOSED SYSTEM

To overcome the drawbacks of the present password systems, we are presenting a robust password scheme, which is multi-platform and easily adaptable for traditional personal computers, smart phones and web applications. Our proposed system has subsystems. The first subsystem is the user registration and the second subsystem is the authentication.

Subsystem 1: where (registration phase) account owner enters his desired username and an alphanumeric password.

Subsystem 2: where (authentication phase) user will be authenticated in 3 steps

Step 1: User enters his username

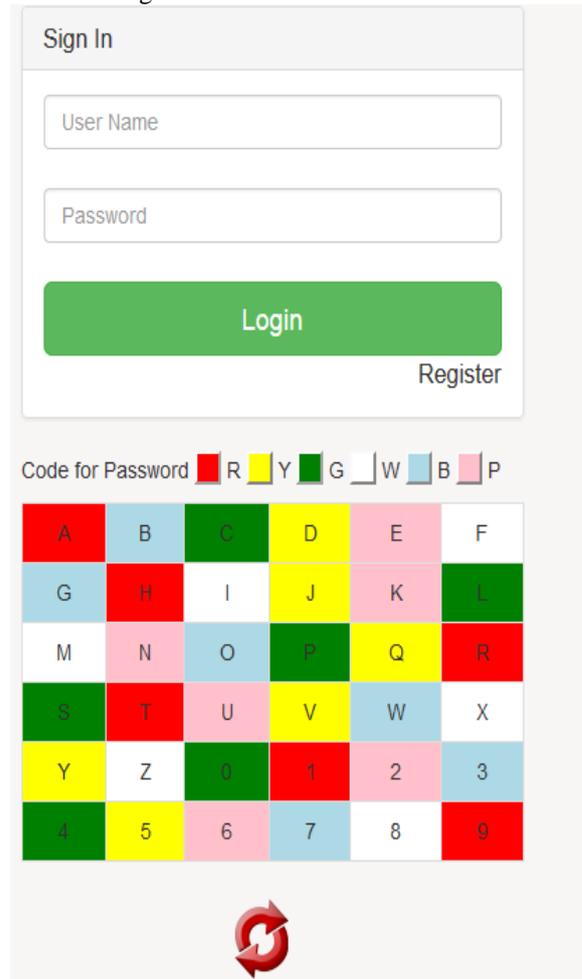
Step 2: A 6*6 color matrix is presented to the user. User has to provide the letter of the background color of grid the first in which his password letters lie

Step 3: In this step identification of the password and security key is done

For every login attempt the background of the box is changed. When the user enters the virtual password, the server verifies the background of the box with given authentication key if it matches the access is given to the user. After refreshing the virtual password expires means the background of the box changes random.

The 6*6color code matrix contains 26 letters and 0-9 digits. The boxes of the matrix are randomly colored using 6 different color sets. The color set contain Red, Blue, Green, Yellow, White and Pink. For each login attempt the colors of the boxes are randomized, the alphabet and digits remain the same as for the convenience of the user. As the user uses the color code matrix password it is impossible for hacker to intrude into your system or knowing password. Somehow the hacker know the color of the box through phishing or some spyware, he never able to identify the original password because the user entering

the virtual password .the user has to choose the good password strength



Code for Password ■ R ■ Y ■ G ■ W ■ B ■ P

| | | | | | |
|---|---|---|---|---|---|
| A | B | C | D | E | F |
| G | H | I | J | K | L |
| M | N | O | P | Q | R |
| S | T | U | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

Fig. 1 A sample line graph using colors which contrast well both on screen and on a black-and-white hardcopy

COLOR CODED ENCRYPTION

converted in ASCII value

ASCII is the abbreviation of American standard code for information interchange it typically based on English, the character are converted into ASCII value

GROUPING THE ASCII VALUE

The converted ASCII values are grouped in four digits, if the character is sort of four digits zeros are added to the last part

ASSIGNING THE COLOR CODE

The each grouped part contains four digit numbers these numbers represent the html color codes, the each part is assigned respective color codes

CONVERTED INTO BINARY VALUES

After assigning the color codes the each color code is converted into binary values

COMPRASSION OF DATA

The converted binary values are too large for transmitting or storing to reduce the size we use XOR to reduce the size of the data

III. CONCLUSION

Authentication is crucial for computer security. As the colour matrix password are attack resistant, there is a growing interest for them. Presently numerous authentication techniques and models are available. But, each of them have their own pros and cons. In this paper we have proposed a color matrix password scheme that is more resilient to dictionary attacks, shoulder surfing, spyware and phishing attacks. This 2 step random colored matrix password authentication scheme shows promise as a usable and memorable authentication mechanism.

REFERENCES

- [1]. Data Compression - DEBRA A. LELEWER and DANIEL S. HIRSCHBERG Department of Information and Computer Science, University of California, Irvine, California 92717 – ACM Journal
- [2]. Lossless Data compression techniques - Klaus Holtz, Eric Holtz, Omni Dimensional Networks , San Francisco , CA 94109 – IEEE Research Paper
- [3]. RGB Coloured Image Encryption Processes Using Several Colored Keys Images - By Rami El Sawda (IEEE senior member) & Habib Hamam (IEEE senior Member) – IEEE Research Paper
- [4]. "Data Can Now Be Stored on Paper" (<http://www.arabnews.com/?page=4§ion=0&article=88962&d=18&m=11&y=2006>) by M. A. Siraj, Arab News (published November 18, 2006)
- [5]. "Store 256GB on an A4 sheet" (<http://www.techworld.com/storage/news/index.cfm?newsID=7424>) by Chris Mellor, Techworld (published November 24, 2006; accessed November 29, 2006)
- [6]. Rainbow Storage, SainulAbideen, Kerala. (Published in November 2006)
- [7]. G. Blonder. Graphical passwords. United States Patent 5559961, 1996.
- [8]. K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.
- [9]. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.
- [10]. Real User Corporation (2007) PassfacesTM, <http://www.realuser.com>.
- [11]. Brostoff S. and Sasse M.A. In People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, U.K, 2000.
- [12]. Sobrado L. and Birget J. (2007) <http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm>.
- [13]. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.
- [14]. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in click-based graphical passwords." in ACM SIGCHI Conference on Human Factors in Computing Systems: Note (CHI), 2010.
- [15]. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
- [16]. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
- [17]. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.
- [18]. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.
- [19]. Renaud, "Evaluating authentication mechanisms," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 6, pp. 103–128. [
- [20]. Herley, P. van Oorschot, and A. Patrick, "Passwords: If Were So Smart, Why Are We Still Using Them?" in Financial Cryptography and Data Security, LNCS 5628, Springer, 2009 Financial Cryptography and Data Security, LNCS 5628, Springer, 2009.