RESEARCH ARTICLE OPEN ACCESS

Color Based Authentication Scheme for Publically Disclosable Entities

A. S. Syed Shahul Hameed*
*(III – Year, UG Student, Department of Computer Science Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Nedungadu, Karaikal - 03)

ABSTRACT
Traditional password authentication system are not strong enough to cope up with the current age of cyber-crime. It's high time that new password authentication schemes are explored and studied. This paper aims to provide an authentication system based on color recognition which would provide a way to encrypt both the username and password. The Color based authentication system would provide an efficient way to encrypt account details for sensitive applications like defense and banking.

Keywords – Authentication, Encryption, Security, Color.

I. INTRODUCTION

With the introduction of internet banking the problem of achieving a secure transaction has always been a concern. The modern age of cyber-crime also triggers the search towards achieving a crack proof encryption scheme for passwords. The most common belief about security is that, it is the password which is the most important entity in all computer applications which has to be safe guarded at any extent. However people tend to ignore the importance of username. People are unaware of the fact that an account is a combination of both username and password. Further, most of the websites and banks educate their customers on how to choose the password and how to safeguard them, but almost no emphasize is given for the username. This turns out to be great fallback in security applications like defense.

To hack any account, the attacker would try to obtain the username first and not the password, which turns out to be a very easy task. It could be very well understood that the first step in hacking is to gain access to the username of the victim. It can also be observed that people, are naturally more susceptible to disclose their username/user-id very easily.

Color based authentication could serve as a viable solution to this generally unattended issue.

II. EXISTING METHODS

The most commonly followed authentication techniques are: Card Based, Biometric Based and Memory Based techniques. The usage of various cards like ATM cards, credit cards, and smart cards comes under the first category. Biometric techniques such as iris scan and finger print are some of the most secure authentication methods under biometric authentication schemes in the world, but with a severe consequence of expensiveness [1]. The installment and maintenance of biometric device requires huge cost. Further, they are unreliable at times. Memory based technique is the most commonly used method. One such memory based technique is text based password, which are being used since olden times. Currently picture based passwords are also in use. The main drawback with this method is, it is extremely prone to human errors.

III. COLOR BASED AUTHENTICATICATION

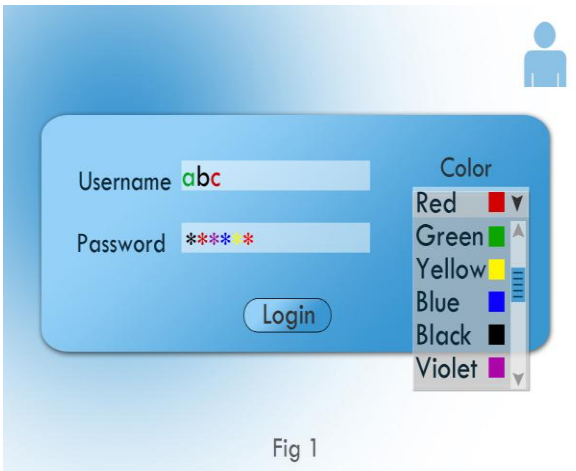
In this authentication scheme an additional layer of encryption is added using color as a parameter for every character in the username and password. When a user fills the login form, for each character he types, he should be prompted to choose a color for it. Essentially the user is associating a color for each and every character he is typing in his username and password. During account registration besides choosing username and password the user should be directed to choose a specific color for each and every character of his username and password.

The text fields for username and password are assigned with a CLR (Color) Listener, which would record the color stroke, the user chooses for each character. This data would be encrypted and sent to the server. The server decrypts this data, and compares it with the data stored in it already. Login attempt succeeds if and only if, both the username, password and the color of each character of the username and password matches.

IV. ALGORITHM

```
Read Username and Password.
Read color stroke of every character.
If (Username AND Password AND color of each
character MATCHES value in server)
Proceed
Stop ().
```

V. DESIGN AND IMPLEMENTATION



Username abc

Password *****

Figure 1: Sample login screen

It could be easily inferred that this scheme of authentication is not so easy and thus not suitable for general uses like social networking. But for sensitive application where security is more important this authentication scheme would serve the purpose.

To implement this scheme of authentication the login screen has to be redesigned to a certain level. An intuitive way has to be provided to the user, so that he can choose the color for every character of his username and password.

Besides the text field for username and password, another field for color has to be provided. The color field has to be coded in such a way that it resets for, every fresh characters the user enters either in his username or password.

One possible user screen is shown in the Fig 1. Here a dropdown box is used to choose the color for each character the user enters.

VI. PRACTICALITY ANALYSIS

The usage of this scheme of authentication by technical experts should not pose any problem and can be very easily incorporated into sensitive areas like defense and industrial applications. Another important aspect is the login time. It could be seen very well that the login time naturally tends to be lengthier in this scheme of authentication. Further, the user has an added responsibility of remembering the color code he chose for each character in his username and password. But this won't be a concern where security prioritizes over time and easiness. Thus it could be concluded that this scheme of authentication is less suited for day to day applications (like e-mails) and more appropriate for banking and defense.

VII. SECURITY ANALYSIS

Now let's explore the various possible methods that are generally employed to break a password.

7.1. Brute Force Search

A conventional text based password has a sufficiently large password space of 94^N [1], where N is the length of password, and 94 is the number of printable characters excluding SPACE. It could be observed that, this itself is a very huge space and only very powerful programs can break a password through this method [1]. But this color based authentication scheme increases the password space several times because the different color for each character itself forms its own password space. Ultimately the password space, in this scheme of authentication would turn out to be (94*K)^N, where K is the number of color options given for the user and N is the length of the password.

7.2. Key logger

Key logger is one of the most commonly used programs by attackers, to steal username and passwords. A well coded basic key logger would stealthily steal the username and password easily. But with this color based scheme of authentication, this problem could be encountered. Though the attacker may gain access to the username and password of the victim there's no way that the attacker can gain knowledge of the color code the victim used for every character in his username and password.

7.3. Shoulder Surfing

Almost all of the text-based password scheme are susceptible to shoulder surfing, which itself is developing as a potentious problem. Though this scheme of authentication is not completely resistant to shoulder surfing it definitely makes things complex for the attacker. It's difficult for the attacker to concentrate on both the character and the color code of each character.

VIII. CONCLUSION

Color based password authentication may provide better security than traditional text based password schemes. It provides an efficient way to protect publically disclosable entities like username. Its best suited for sensitive applications like defense and banking. To make this scheme complete, much more research and studies are needed for a successful implementation.

IX. ACKNOWLEDGEMENTS

I wish to thank my mother for her continuous support through this paper. I would like to express my gratitude to professor Maneckshaw. B (Department of Mathematics, Karaikal Polytechnic College) for recognising my idea, and helping me for completing this paper. I would also like to thank my brother-in-law Mr. R. Shaik Ali Maricair for helping me to prepare the image resource for this paper.

REFERENCES

[1] ARUN PRAKASH. M., GOKUL. T.R., 2011 Network Security-Overcome Password Hacking Through Graphical Password Authentication. *Proceedings of the National Conference on Innovations in Emerging Technology-2011* Kongu Engineering College, Perundurai, Erode, Tamilnadu, India.17 & 18 February, 2011.pp.43-48.

[2] BIRGET, J., HONG, D., AND MEMON, N. 2003. Robust discretization, with an application to graphical passwords. *Cryptology ePrint Archive*, Report 2003/168.