ISSN 2229-5518

Improved Password Selection Method to Prevent Data Thefts

Akash Mathur

Abstract— Password thefts have become an important data security issue in the recent times. Hackers have been intruding into the websites and personal mail accounts of the users. Prevention from this unauthorized access is the need of the hour. So here lies the major key to overcome such a situation and that is to adopt more secure and advanced password selection methods. My paper throws light on one of the most secure methods to improve password strength and security.

Index Terms— Password selection, Data security, Prevention data thefts, Cyber security, Password, Prevention from hacks.

1 INTRODUCTION

THIS is the era of globalization. Every part of the world is potentially connected to the other part. The data travelling has become so easy that it takes only a few seconds for the exchange of media. But with the advancement of the worldwide internet the security of the data is an important issue. How secure is the data is an important issue. Data threats are now common, password hacks being the most common ones. Severe vulnerable attacks on websites had leaded its users to suffer a huge discomfort. Majority of steps are now employed to protect data from theft but how effective are they is an important issue. E-mail websites have been majorly affected by the improper password selection and mismanagement problem. This has resulted in unauthorized entry to the user's personal account. The password strength also is not capable enough to counter the security issues.

Since my main interest has been the web securities I decided to focus on the password selection process.

The main aim of this paper is to lay stress on the security issues related to password selection and management. The idea is to provide the users of the websites an option to choose the password along with their font color.

The passwords must not only comply with at least 6 characters scheme but also color coding pattern can prove to be beneficial. Basic colors including black, red, and white can be adopted to double protect the password. The main idea is that the user not only types the password in the password field box but also selects basic colors of the fonts too used in the password. The ASCII codes used in the password field should be merged with the color combination. The website designers should employ coding to merge the text passwords with font colors to reduce security threats and identity thefts. The credit card owners can be saved from frauds which are caused due to unauthorized access by the stealing computer programs. This unauthorized access can be prevented by using colored alphanumeric passwords. The basic colors of red, black and white won't increase the size of the website and would also not slow down the identification process on the websites.

ADVANTAGES

The advantages of using color implemented password fields are:

- With HTML coding, the password box must also support colored fonts i.e., color coding [1] for better security. There should be a blend of both characters and colors when used as a password.
- Virtual keyboard [2] can also be made into use by making it color adaptable. Many times virtual keyboard helps to protect the accounts from hacking programs. Therefore virtual keyboard should also be designed which support colored fonts when typing password in the password field.
- Hacking programs [3] which record the keyboard hits also known as key loggers [4] also fail since color combination requires mouse clicks and visualization eye of the user. Therefore once again the login process has high security especially E-mail hacking [5] will be reduced to great extent.
- Hacking issues can be minimized to a great extent. Even if multiple hacking programs run, but it is only the eye of the user which can see the color of the password font. So now users will be safer in terms of password management.
- Guessing attacks are also reduced, since guessing colored font password seems to be impossible

COMPLICATIONS

The complications accompanying color implemented password scheme are:

- The size of the website may increase. Website

size becomes heavy on using colored fonts in password fields.

- User interface may become unfriendly. Users might take some time to adapt to this pattern.
- Website hosting price increases with the increase in no. of bytes. If the websites increase in size using this technique, then the cost of hosting would definitely increase.
- One of the shortcomings can be that the identification process of the websites [6] can be slow during the login process.

MEASURES ADOPTABLE TO OVERCOME COMPLICATIONS

The following are the measures which can be adopted to overcome the complications:

- Use of only basic 3 colors red, black and white won't increase much size of the website. Since use of more than these colors would increase the size and consequently the website host prices.
- Graphically adaptable user interface can be used without increasing much of the website size. Skilled website programmers can make the user interface more convenient and user friendly without slowing down the processing of the websites.
- Website hosting prices increases but the security issue solves to a great extent. Data is now more secured with this color coding technique. Even the key loggers fail to track the typed password
- Website's identification process won't be very slow since only basic colors like red, black and white are used as colors for fonts which won't increase much the size of login page and will offer higher security to the users.

BASIC IDEA INTERPRETATION

The following figure correctly interprets the situation after the color coding pattern for password field is adopted and embedded in the websites.

USERNAME:	abcde
DEFINED PASSWORD:	123abc
COLOR CODING: 	
FINAL PASSWORD:	123abc or 123abc or 123abc

Figure 1. Login format after use of technique

Assume the figure above as the login page of a website then, various color combinations can be used to set the final password.

CONCLUSION

To secure the data on the web, implementation of such a system of colored font passwords is an essence. Use of at least 6 text or alphanumeric characters with colored fonts as password in the password field makes its strength increase many folds. Protection of user accounts like that of E-mail and credit cards from hackers are some of the advantages of using such system. Prevention from identity thefts is also an added advantage. These color combinations technique provides highly secured gateway for the exchange of data on the internet. Although this might seem to be a complicated password selection procedure but is highly effective and secured method, once adopted and embedded with the websites. Even the hacking programs fail when such a system of password selection and management procedure is implemented.

ACKNOWLEDGMENT

I would like to thank my dad, mom and brother for supporting me and having faith on my research aptitude.

REFERENCES

[1] L Cottrell, L M. Cottrell, "*HTML & XHTML Demystified*", USA: The McGraw Hill Companies, pp. 50-56, 2011.

[2] M Hirose, "*Human-Computer Interaction INTERACT '01,*" *Netherlands: IOS Press*, pp. 678-679, 2001.

[3] S Mclure, J Scambray, G Kurtz, "*Hacking Exposed". 5th* Ed. USA: McGraw-Hill/Osborne, 2005.

[4] R.C Newman, "*Computer Security: Protecting Digital Resources",* Jones and Bartletts publishers, pp. 58-59, 2009.

[5] A. Fadia, "*Email Hacking". 2nd Ed.* India: Vikas publishing house pvt ltd, 2009.

[6] M Kimwele, W M Wangi, S Kimani, "Strengths of a colored graphical Password Scheme," *International Journal of Reviews in Computing,* vol 4, pp. 64-65, Oct. 2010.