IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Graphical Password Authentication

[1] Ishwar Padade, [2] Manoj Parate , [3] Sanket Gharde, [4] Mithil Wasnik

[1, 2, 3, 4] Department of Computer Technology,RTMNU, Rajiv Gandhi College Of Engineering And Research, Nagpur, Maharashtra, India.

Abstract - Graphical passwords are termed to be a secret or secure means that a user inputs to the system by the means of computer's graphics, it may be by mouse, stylus as inputs devices and output devices. The most terms of computer security or in the process of authentication is text based passwords i.e. the typical traditional method is "User name" and "Text based passwords". The conventional methods of authentication or genuineness is to use text based or alphanumeric user names and password, the Graphical passwords are the alternatives or the substitutes of the conventional alphanumeric passwords, as comprehensive study and researches have proved that the human tends to remember and recognize images better, it is comparatively easier to remember the geometric figures, colors, shapes, patterns, textures compared to the conventional and traditional text based passwords. The graphical password techniques are classified into two broad categories: recognition-based and recall-based approaches. The operations and highlighted aspects of the system are explored as it tends to provide more resilient passwords for information security.

Keywords **- Usability, Security, Graphical Password, Authentication, password security.**

1. Introduction

In today's world the authentication play vital role in computer security. It tells how to control and handle user accounts [1]. Today there are many types of user authentication system available and used but the alphanumerical username and password are one of mostly used type of authentication scheme. This scheme is very easy to understand and implement and also easy to used. The alphanumerical password is the combination of alphabets and numeric value (digits), it easy for the user to remember but hard for others [2]. But these password can be easily hack by the hacker or it can easy target of dictionary attack [3 ,4]. So that user can make a password which is very difficult to guess for others and we write it on paper which can be known to others [5].

For these reason several techniques are invented to overcome the limitation of alphanumeric password. One invention is that easy to remember the long phrases (passphrase) rather than password as a short length [6]. This is very lenthy technique. Another technique is to use graphical password, in which the user will choose the image as a password than alphanumerical password [7]. In this technique user will select one or more than one picture and select the region on the picture rather than typing a alphanumerical password. Graphical password scheme provides a possible acceptable alternative for text based scheme, motivated by the fact that human tend to remember picture better than text [8]. Picture, colors, textures, patterns, shapes, figures are generally easy to remember or recognized than text.

2. Graphical Password

Graphical password is the picture as a password. Human remember picture immediately and long time rather than words [8], it is also difficult to break. The memorability of the image is because of its nature and specific sequence of click locations ,undertake to retrieve the password. Image with meaningful content will supports the users memorability.

The graphical password technique are devided into two broad categories [7]:

- Recognition based
- Recall based

In recognition based technique a user is considered genuine or authenticated by provocations or by challenging to identify that images that he had selected during the registration phase [9].

In recall based technique the user is asked to create something that he had created or selected earlier in the initial phase. An early recall based technique was introduced by Greg Blonder in 1996 [10]

2.1 Proposed Work

The proposed graphical authentication systems are work as follows:

In our system, the user has to register himself in system first by putting his name in username field and other field present in the registration form and choose the picture for

password. The user will select several regions on the picture he or she interested in it. Each region he or she selected as a password is describe by rectangle. During the selecting the every region the message will generated i.e. after selecting the first region the message "first point is selected" will generate and respectively for all points. If user doesnt select any point then also message will generated.

In figure 1, we show the example of user creating his graphical password. In this example user puts his username in username field and check for availability and one message will display e.g. "User Is Available" and if the user will already available then user has to register with another name. after checking of availability user will select which type of image he has to selected e.g. single image or multiple image and respected image type will display by the user from browse and also select number of points on the image. After selecting points on the image user has to select one security question in security question field and write its answer. The security question field is for recovery in the case if user forgot his password, then by giving the answer of security question user can recover his password. After filling allthe field in registration field user will click on submit button and user will register. All information will save in database. In multiple image type, user will select multiple images as shown in figure 2, and select one region on every region and follow every step same as in single image. In login screen, the user will type his username in username field and click on check availability if the user will already available then one message will display e.g."User Is Already Available" and respective image will automatically display on picture box which is already save in database. In our proposed system, user can free to choose the image and select points on it and he can reset it and recover it in case of forgot the points on it. In reset login screen as shown in figure 4, by giving the answer of security question correctly user can recover his password.

3. Figures

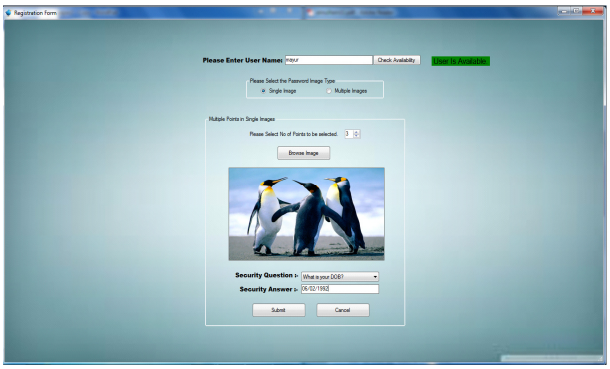

Figure 1: Single Image

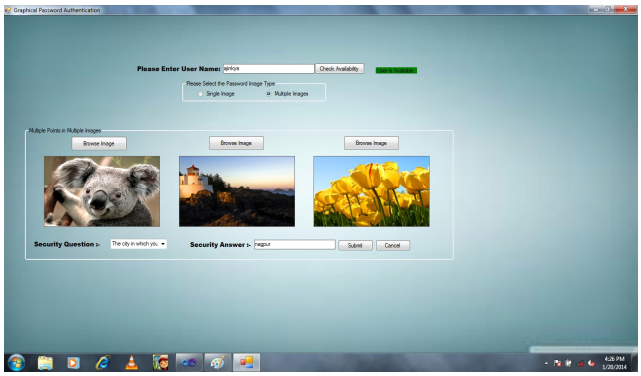

Figure 2: Multiple Image

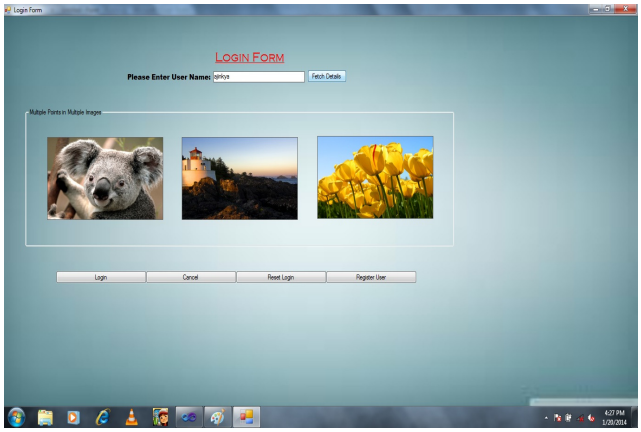

Figure 3: Login Screen

4. Conclusions

Now a day's, authentication is the main part of computer security. In our proposed system we proposed graphical password authentication mechanism by considering the users ability to recognize the images. The main argument password is that people are better at memorizing graphical password rather than text based password. The analysis suggest that it is more difficult to break the graphical 2password using the traditional attack method such as dictionary attack or spyware. We can also provide a virtual keypad through which password can be entered and can define some special characters in the character set for text passwords. For graphical passwords we can draw images or symbols on the virtual screen and can use those images as passwords.

References

[1] William Stallings and Lawrie Brown. Computer security: Principle and Practices. Pearson Education, 2008.

[2] Susan Wiedenbeck, Jim Waters, Jean-camille birget. A lex Brodskiy, and Nasir Memon. Passpoint: design and longitudinal evaluation of a graphical password system . International journal of Human-Computer Studies,63:102, July 2005.

[3] Robert Morries and Ken Thompson. Password security: a case history. Communication of the ACM, 22:594-597, November 1979.

[4] Daniel V.Klein. Foilling the Cracker. A Survey of, and Improvement to, Password Security. In proceedings of the 2nd USENIX UNIX Security Workshop, 1990.

[5] Eugene H. Spafford. Obseving reusable password choices. In Procceding of the 3rd Security Symposium Usenix, page 229-312, 1992.

[6] Sigmund N. Porter. A Password extension for improve human factor. Computer & Security, 1(1):54-56, 1982.

[7] Xiaoyuan Suo,YING Zhu, and G. Scottt Owen. Graphical Password: A survey. In Proceeding of Annual Computer Security Application Conference, pages 463-472,2005.

[8] Antonella DE Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand word? Exploring the feasiblility of graphical authentication system. International Journal of Human-Computer Studies, 63:128-152,july 2005.

[9] Real User Corporation. The science behind passfaces, june 2004.

[10] G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill,NJ),August 1995.