Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Graphical Password Authentication Mechanism

Delphin Raj K M
Assistant Professor
MEA Engineering College
Perinthalmanna, Kerala, India

Nancy Victor
Assistant Professor
VIT University
Vellore, Tamilnadu, India

Abstract— Authentication can be defined as the process by which the identity of the user is verified to determine whether the party is, in fact, who it claims to be. The most common authentication mechanism involves the use of alphanumeric passwords. But, alphanumeric passwords are easy to guess and they are not secure. Graphical passwords comprises of giving images as passwords. Different graphical password schemes are employed for providing better security. This paper focuses on a novel authentication mechanism using various techniques for providing security. This authentication mechanism involves alphanumeric passwords, images as passwords, CATCHA and also a random number generator for security purposes.

Keywords— Alphanumeric Passwords, Authentication, Captcha, Graphical passwords, Random Number Generator.

I. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. One of the major areas where human computer interaction is important is authentication. Username and password combinations are used for logging in into any application. A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource. The password should be kept secret from those not allowed access. It is the duty of the individual to keep the password secure. But, humans tend to choose passwords which are easy to guess; i.e. person's name pet's name, date of birth, phrases etc. At the same time, this password is easy to guess for the attacker also. To address the problems with traditional username password authentication, other authentication techniques like biometrics and graphical passwords can be used.

The general text password vulnerabilities include shoulder surfing, dictionary attacks, user error, limited password space for text, uses plain words (other than jumble of characters), users choosing guessable password or write then down etc..

Graphical passwords may be a solution to the text based password vulnerabilities. A graphical password is an **authentication** system that works by having the user select from **image**s, in a specific order, presented in a graphical user interface (**GUI**). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).The idea of graphical passwords was pioneered by Greg Blonder who also holds the US patent 5559961.A graphical password is a secret that a human user inputs to a computer with the aid of the computers' graphical input (e.g., mouse, stylus, or touch screen) and output devices. Here the user uses visual recollection in order to gain authentication to a system. Therefore the human factor in securing information is limited.

The Graphical Password technique was designed to meet the basic and advanced requirements of an authentication system. Graphical Password implements basic requirement like authentication. This can be implemented at individual level, and also at institution level. As human beings have the ability to remember pictures easily, this method will make the authentication process much easier to an extent. Because of these advantages, there is a growing interest in graphical password. In addition to workstations and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

This paper focuses on a novel authentication mechanism using various techniques for providing security. This authentication mechanism involves alphanumeric passwords, images as passwords, CAPTCHA and also a random number generator for security purposes.

II. LITERATURE SURVEY

This chapter mainly focuses on the various authentication schemes already available. It includes alphanumeric passwords, graphical passwords and CAPTCHA.

A. Alphanumeric Passwords

Alpha-numeric passwords are the most commonly used authentication mechanism [1]. This scheme was first introduced in 1960's. This was introduced as a solution to the security issue that was facing at that time. These are just a string of letters and digits. This technique offers a good security mechanism. They cannot be simply deduced or guessed. There are some commonly used guidelines for setting a good alphanumeric password, which is easy to imagine or break.

i. Length of the passwords should be at least 8 characters.
ii. The password should not be easy to relate to the user (e.g., last name, birth date).
iii. It is recommended that the password should not be a word that can be found in dictionary or directory.
iv. Ideally, the user should combine upper and lower case letters and digits.

The best password should be always a completely random one. Some techniques for creating pseudo random passwords were also devised by humans. This includes taking a common word and doing some random operations on it. This normally includes having a mixture of upper case and lower case letters, either by alternately using it or by having the first half of the words in uppercase and next half in lower case and vice versa. Another method includes jumbling the word randomly. Yet another approach is by simply reversing the string for creating a password. Another method involves combining the year of birth or current year along with the password that they are creating.

A major drawback of using alpha numeric password is the dictionary attack [2]. This mainly happens when user selects a password which is available in the dictionary. There are various mechanisms by which the passwords can be cracked easily assuming that the password is a word that appears in the dictionary. This attack is mainly for finding out the valid passwords of some users of a given system.

B. Graphical Passwords

Graphical passwords were originally described by Blonder (1996). Graphical passwords provide better security when compared with normal alpha numeric passwords [3]. Graphical passwords provide a new way of setting the password using images. An image or a set of images can be given for the user. The user is asked to select a portion of the image. If he is able to provide the exact region of the image that he has given during setting the password, the user will be authenticated to use the application..

Since users are able to remember only a set of alphanumeric passwords, they have the tendency to note down the passwords and also to choose passwords that is related to the application that they are using [4]. A picture is worth a thousand words. As this statement stands true, the user can remember images better than mere alphanumeric text. Choosing the locations that needs to be set as the password, depends on the image itself. Click locations also depends on the nature of the image.

There are mainly two types of Graphical Password Authentication Mechanisms [5].

i. Recognition based graphical technique
ii. Recall based graphical technique

In Recognition based systems, the user will be asked to select the image that he has selected during setting the password, from a set of images. If he is able to identify the image correctly, he will be authenticated. One of the techniques is employing pass faces. Another technique is employing pass objects.

In Recall based graphical systems, the user will be asked to reproduce something that he has created while setting the password. DAS (Draw a Secret) is one of the techniques employed with this system.

As there are no pre-existing dictionaries for graphical information, dictionary attacks are infeasible. The password space is also quite large. Humans can remember a person's face or object in seconds, a computer takes some considerable amount of time for the same. The table below shows some of the graphical password schemes used and the authentication process it follows.

TABLE 1

Graphical Password Scheme	Authentication Process
Pass Faces	Identify and select images given during setting the password
Pass Objects	Click a specified area given during registering the password
DAS	Users draw the graph on 2D grid
Pass Clicks	Click locations of a picture in the right sequence

C. CAPTCHA

The term CAPTCHA (for Completely Automated Public Turing Test to Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University.

A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. CAPTCHA implementations are currently divided into three categories [6]:

i. Visual programs based on OCR (Optical Character Recognition) problems
ii. Visual programs based on non-OCR problems
iii. Non- visual programs

III. EXPERIMENTAL RESULTS

Graphical passwords were originally described by Blonder. In his description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known.

Recognition is an easier memory task than pure, unaided recall. In our password system we use a three level authentication scheme. In the first level, the user will be asked for retrieving an image which he has chosen as the password. If he gives this password correctly, then he will be asked to select certain numbers which he has chosen while creating the account, from a list of rolling numbers. After this second level of authentication, he will have to provide a textual password as the third level. Also, the user will be asked to enter the CAPTCHA correctly. Only three chances will be given for this final phase. If he goes wrong, he can try only after 5 hours. For this, timestamp also can be employed. If he is able to pass these three levels without any difficulty, he will be able to enter the application. This scheme actually employs click based and choice based approaches [7].

The click based approach used here actually employs selecting an image from a set of images. It can be either a set of human faces or a set of object images. The choice based approach needs the user to select a sequence of images. After the image is selected, again a recall based approach should be followed to identify the portion of the image he has selected during the password setting phase. Instead of these methods, a DAS method also can be used for setting the password. The technique of cued recall allows the users to reproduce a drawing with some set of hints to support the user. There are various steps for setting the password.

The rolling numbers used in this approach also helps the user to recollect something that he has given as the password. So, the entire approach used here is mere recall and recognition based. The CAPTCHA used here is just for ensuring that a human is actually using the application. Using all these techniques which is having some specific functionality, the scheme proposed here stands to be a very good authentication mechanism. The scheme proposed here can be used for better network security also. Password hacking is really difficult with this approach. The shoulder surfing resistant password scheme is the best authentication method that can be used.

The entire process of setting the password is explained in the following figure.

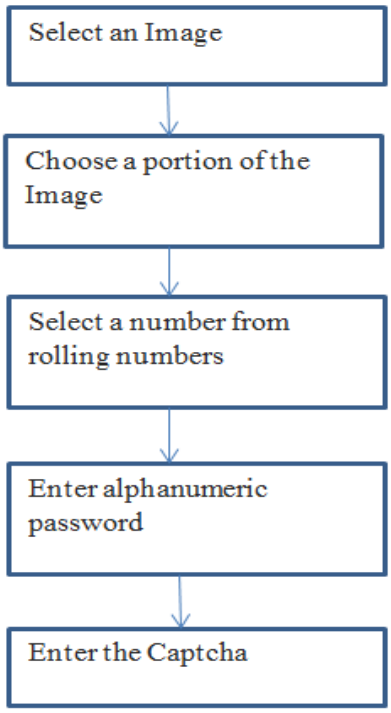

Fig. 1 Setting the Password

The first phase of setting the password involves choosing an image from a set of images. After the image is selected, the user will be asked to select a particular portion of the image to be set as the password. The pixel positions are stored then, and will be used for checking the password when the user enters the graphical password. Actually, a rectangular portion will be selected as the password, and hence the coordinates of the rectangular portion should be saved by the application.

During login procedure, when the user clicks on any portion inside the image, he will be directed to the next phase. It is always recommended to have only a small rectangular portion to be made as the password as it offers better security than the normal procedure. After this phase of setting the password, a new window is given where a set of rolling numbers will be there. Two options are provided for this phase. One includes pressing the start button, which then starts displaying the numbers randomly. Second option allows the user to insert a particular number from the rolling list of numbers.

Once these two phases are successfully completed, the user will be provided with a set of images with some random numbers displayed on top of it. At first, the user has to select the correct image with the random rolling number combination that you have chosen during the first two phases of setting the password. If this image-random number combination turns out to be the same combination that we have used, the user will be asked to choose a username and password combination which consists of alphanumeric characters. Finally, the user will be asked to correctly enter the captcha that is provided.

The following figures well explain the complete concept of setting the password using the Graphical Password Scheme.

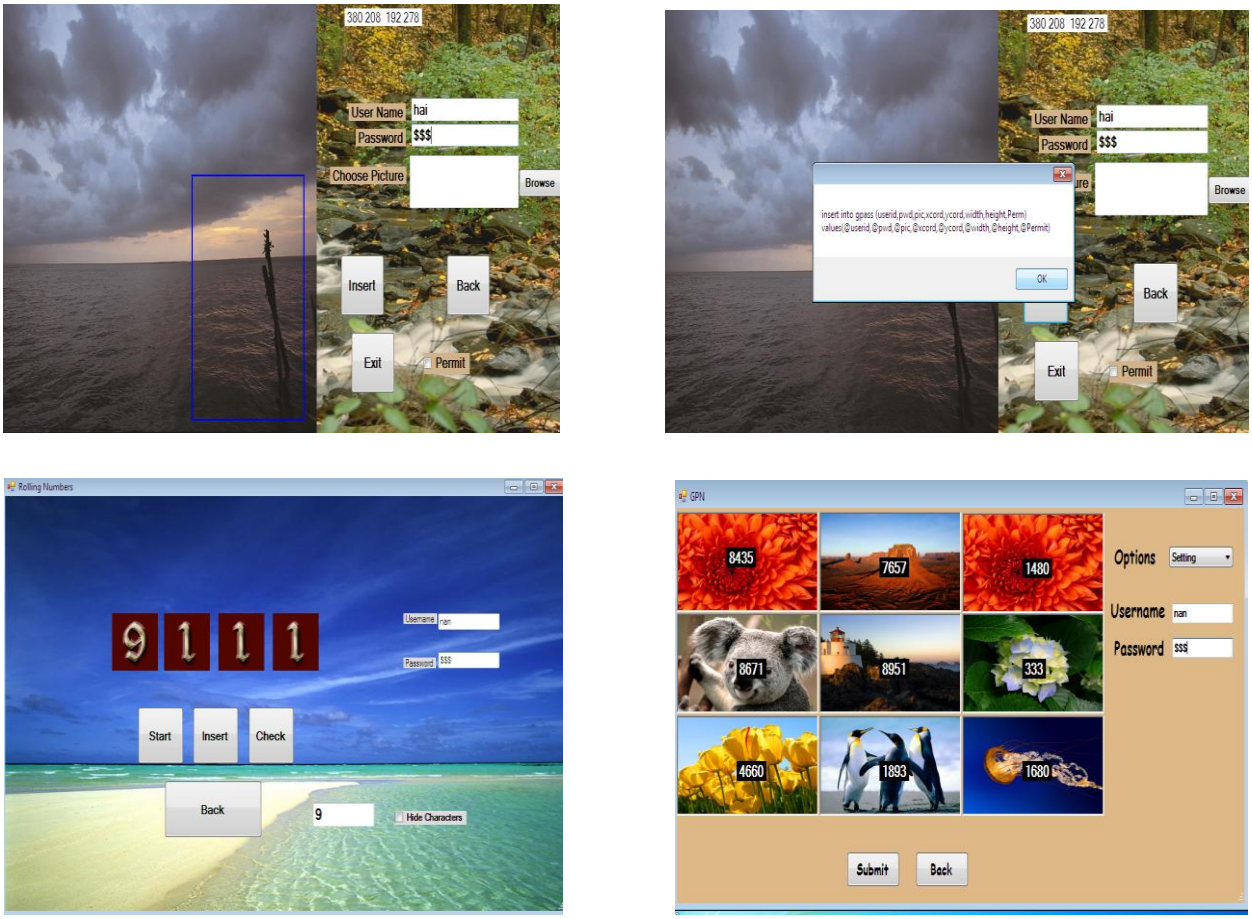

Fig. 2: The Different Phases of Setting the Password

For accessing an application, the user has to pass through all these phases correctly. As the first phase, the user will be given a set of images. He has to first select the correct image. After that, he will be asked to choose the portion of the image that he has given as the graphical password. Once he has completed this first phase of the password, he will be asked to choose the number he has given while setting the password, from a rolling set of numbers. Then, as the third phase he will be asked to enter the correct alphanumeric username password combination. Finally, the user will be asked to enter the captcha also to ensure that the application is going to be used by a human only.

For choosing the graphical password, the user can adopt any technique. The application can have a recall based password or a recognition based password depending up on the application they choose. The application can make use of a set of pass faces for the same. It is not necessary that the image selection should have images consisting of human faces alone. Any image can be given depending up on the user's interest. Personalization also can be done for better security.

IV. CONCLUSIONS

This paper focuses on a novel graphical password authentication mechanism which involves four different phases of setting the password. The four phases include choosing an image for setting the password, choosing a part of the image, choosing a number from a set of rolling numbers, choosing an alpha numeric password and finally, entering a CAPTCHA correctly. As it combines both images and alphanumeric text, this scheme has the best in both the approaches [9]. Future Enhancements include using a combination of all recognition based systems for better security. Also, as an additional security mechanism, biometric system also can be implemented. A hand written password is another option for enhancing the scheme [10]. Network security hacking problems also can be reduced to a great extend if we are employing this Graphical Password authentication mechanism.

REFERENCES

[1] Huanyu Zhao and Xiaolin Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 0-7695-2847-3/07 $20.00 © 2007 IEEE.

[2] Steven M. Bellovin, Michael Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", 0-8186-2825-1 /92 $3.00 d 1992 IEEE.

[3] Wei Hu,Xiaoping Wu, Guoheng Wei, "The Security Analysis of Graphical Passwords ",978-0-7695-4260-7/10 $26.00 © 2010 IEEE.

[4] Ali Mohamed Eljetlawi, Norafida Ithnin, "Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods", Third 2008 International Conference on Convergence and Hybrid Information Technology, 978-0-7695-3407-7/08 $25.00 © 2008 IEEE.

[5] Wei Hu,Xiaoping Wu, Guoheng Wei, "The Security Analysis of Graphical Passwords ",2010 International Conference on Communications and Intelligence Information Security, 978-0-7695-4260-7/10 $26.00 © 2010 IEEE.

[6] Mohammad Shirali-Shahreza, "Highlighting CAPTCHA", 1-4244-1543-8/08/$25.00 ©2008 IEEE.

[7] Yuxin Meng, "Designing Click-Draw Based Graphical Password Scheme for Better Authentication", 978-0-7695-4722-0/12 $26.00 © 2012 IEEE.

[8] M.ArunPrakash, T.R.Gokul, "Network Security-Overcome Password Hacking Through Graphical Password Authentication ", 978-1-61284-810-5/11/$26.00 ©2011 IEEE.

[9] Ahmad Almulhem, "A Graphical Password Authentication System", 978-0-9564263-7/6/$25.00©2011 IEEE.

[10] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, PoulamiDas, "User Authentication by Secured Graphical Password Implementation", 978-4-88552-226-0/08/$25.00©2008 IEICE.

