ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Captcha as a Graphical Password Authentication System (CaRP)

[1] Archi Gaikwad, [2] Bijal Parekh, [3] Medha Kona [4]Shweta Bramhane
[1][2][3] Department of Information Technology
Yeshwantrao Chavan College of Engineering

***Abstract* - We face many security breaching issues for our desktop applications and online services. Many internet applications commonly use text based passwords for authentication. Text based passwords are prone to many attacks such as online guessing attacks , relay attacks ,shoulder surfing and are usually hard to remember. Graphical password proves to be a much better alternative to overcome these attacks. This paper introduces the use of Captcha as Graphical Password- CaRP to enhance the security at the time of login. CaRP is the combination of both graphical password and captcha technology. This system allows the user to select different visual login schemes. CaRP is one of the reasonable solutions that provides added security.**

***Keywords:*--- Captcha, CaRP , hotspot, dictionary attack, Graphical password password guessing attack, security primitive.**

I. INTRODUCTION

To keep the computers secure and to authenticate users, text based passwords are generally used. Long and random passwords provide added security but since they are difficult to remember, users tend to use passwords which are short and common which makes the system vulnerable to various attacks. The most common attacks include online guessing attack, relay attack, shoulder surfing, dictionary attack, etc. The two major goals of any password authentication system must include the use of strong passwords while maintaining the remembrance of the password.

1.1 What is CAPTCHA ?

Captcha is defined as completely automated public turing tests to tell computer and human apart. The distorted image that can be recognized by a human is generated by captcha. Since extraction of the text from a distorted image is difficult for a computer, captcha is used which is easily understood by a human user.

1.2 Captcha as Graphical Password (CaRP)

The combination of two technologies namely, graphical passwords and captcha technology gives us CaRP system. The generation of CaRP makes use of alphanumeric characters. The password in a CaRP image is created by clicking the points on that image. The CaRP system generates new image for attempt made to log into the system. The sequence of the click points chosen by the user is of utmost importance.

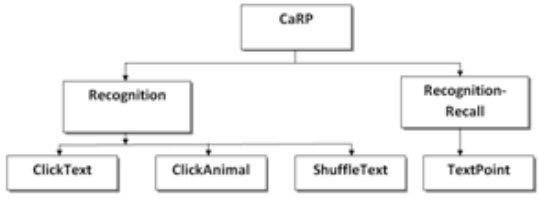


Figure 1: Detailed Scheme of CaRP[3]

II. CAPTCHA SCHEMES

The various captcha schemes used in this paper are defined as follows :

2.1. Scheme 1- Click Text

This is a detection based scheme with CaRP property. This scheme involves randomly arranged characters in CaRP challenge image. Basic thumb rule is that challenge image should not contain any visual complicated characters like as “0” and “O” alphabet. Basic CaRP challenge image for ClickText is shown in Figure 3. Following are steps for this scheme:

Step 1: User registers on system by giving details along with username and password. This password is sequence of alphabets. e.g. P = “KBDAY”.

Step 2: When user needs to login to the system with Click Text Scheme, then user has to provide username. User will get CaRP challenge image form by captcha engine to provide click-based password. This challenge image is nothing but randomly arranged alphabets.

Step 3: User click on alphabets occur in CaRP challenge image. Here to provide proper login password, user has to click on alphabets refers to password string i.e. P = “KBDAY”. Here click sequence is essential.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Step 4: While creating CaRP challenge image synchronize of each alphabet is recorded. When user click on alphabets these provided co-ordinates is send to the server. Server then gets letters from co-ordinates. String from these letters is formed and matched with authentic string of password.
Step 5: If username and password matched then user will redirect to next page else user will redirect to login page again

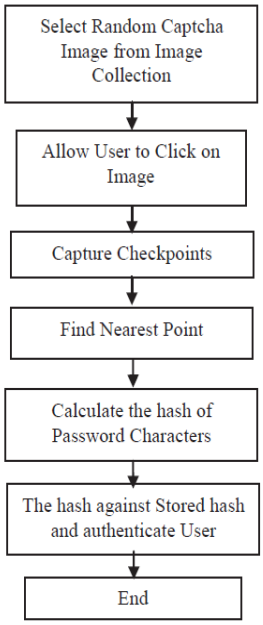


Figure 2: Flow chart of CaRP authentication[2]

Figure 3 : Click Text CaRP[2]

2.2. Scheme 2 - Text Points

This is a detection-recall based scheme. In this scheme, to insert a key, a user must trace the click points in a CaRP challenged image, and click the uniform points matching the password. In this case uniform point means a point in particular alphabet that has a stable relative position in different fonts. User has to provide arrangement of such uniform points by choosing particular alphabet at time of registration. When user wants to login then he will get CaRP challenge image consist of registered alphabet. User has to trace and click approximate positions in alphabet which he used at time of registration. Following are steps for Text Points:

Step 1: At time of registration user select alphabet and select string of uniform points as a password shown in Figure. 4 (in red color). Authentication server stores user details along with password hash value containing alphabet and respective uniform point co-ordinates as original details.

Step 2: When user try to login then he has to give username along with he has to copy uniform points which is password sequence shown in Figure. 4

Step3: Authentication server matches these point sequence with original credentials. If these point string is as expected then user will be authenticated else user will switch to login page again. Figure. 4 Text Points CaRP challenge image. Here following are some precautions to be taken while performing image processing and generation of CaRP challenge image. x While generating this CaRP challenge image, clickable points are kept independent and care is taken that they should not overlay. The resistance region should not be overlay. At time of authentication user clicks represents grid-cells. If clicks are within resistance then it is true. This grid-cell sequence accomplish by user clicks is matched with genuine password i.e. genuine grid-cell sequence given at time of registration.

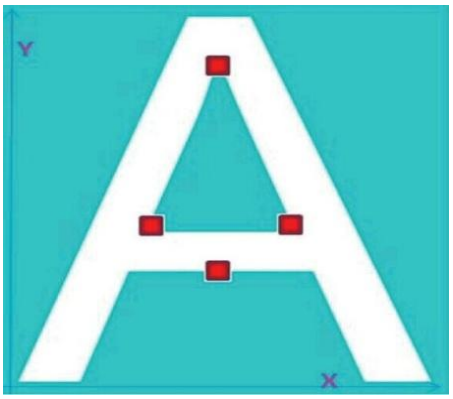


Figure 4 : Text Points[3]

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

2.3. Scheme 3 - Click Animal

This is a recognition based scheme. In this scheme, to enter a password, a user must trace the sequence points in a CaRP challenged image, and click the invariant points matching the password. In this case invariant point means a point on particular animal that has a fixed relative position in different fonts. User has to provide sequence of such invariant points by selecting particular alphabet at time of registration. When user wants to login then he will get CaRP challenge image containing registered animal. User has to trace and click relative positions in alphabet which he used at time of registration.

Following are steps for Click Animal:

Step 1: At time of registration user select an animal and select sequence of invariant points . Authentication server stores user details along with password hash value containing animal and respective invariant point co-ordinates as authentic details.

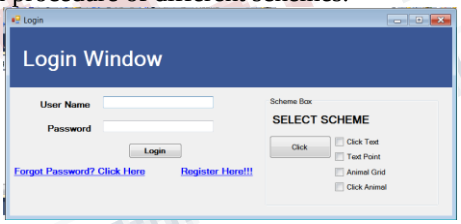
Step 2: When user try to login then he has to provide username along with he has to imitate invariant points which is password sequence .

Step 3: Authentication server matches these point sequence with authentic details. If these point sequence is as expected then user will be authenticated else user will redirect to login page again.

III. IMPLEMENTATION

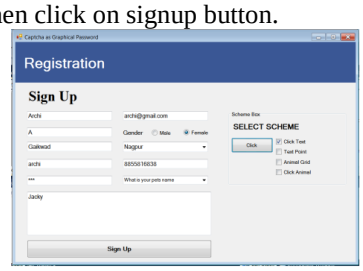
1.Home Screen

The home screen comprises of Registration form for new user and login window for registered user. And selection procedure of different schemes.



2. Registration Form

A new user needs to fill a simple registration form in order to access the system. The registration form comprises of simple fields that need to be filled by the user and then click on signup button.

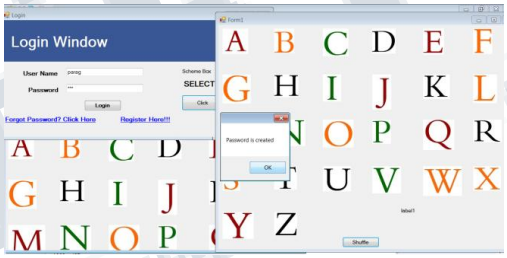


3. Scheme 1: Click Text

The user need to select the scheme that one wants to access or through which one would like to enter into the system. The first scheme is ClickText , user need to click on checkbox placed before ClickText caption.

4. Password Generated

In ClickText, the user need to select the alphabets as password upto 5 character length. Then, the password will be generated and stored in the database.

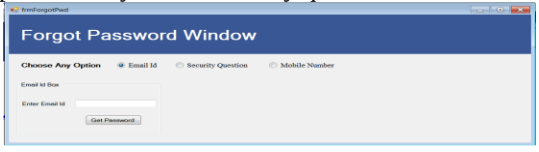


5. Click Animal

In click animal, user needs to select an animal from the grid of animals. And then user need to select invariant points on that particular image ,and image and points of that particular username will be stored in database.

6. Password Recovery using email

In case an unauthorized user tries to open ones account , then the account will get locked , if the image and point selection is wrong. Then the authorized user can recover the account using three different techniques i.e, recovery of password by email, security question and mobile number.

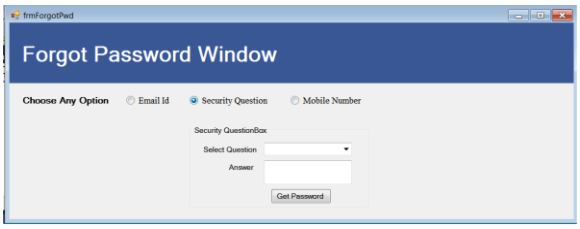


ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

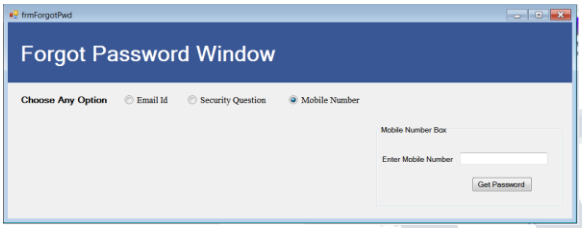
7. Password Recovery using Security Question

In this recovery option , authorized user need to select the security question that he choose at the time of registration phase and need to specify the correct answer that he/she provided at the registration time. Then account will be recovered.



8. Password Recovery using Mobile Number

The authorized user need to provide their mobile number ,then recovery code will be provided on their mobile number to unlock the account.



IV. CONCLUSION

In this paper, security schemes are stated. CaRP, a new security system which provides solutions for various online attacks. This is nothing but a new graphical password technique which combines with new approach called Captcha. This technique is used while every login attempt to make sure system is independent of online guessing attacks. This password technique is very difficult to hack passwords generated by CaRP. CaRP is found probabilistically. It also helps to resort many other attacks like Captcha relay attacks, shoulder-surfing attacks. In this, the schemes introduces are Text Point, Click Text, Click Animal. These techniques are easier to use than any other techniques. This scheme has better remembrance than traditional password schemes. CaRP has good potential for making quality password system.

REFERENCES

[1] Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

[2] The Graphical Security System by using CaRP. 2015 International Conference on Energy Systems and Applications (ICESA 2015) Dr. D. Y. Patil Institute of Engineering and Technology, Pune, India 30 Oct - 01 Nov, 2015.

[3] Click and session based - Captcha as Graphical Password Authentication Scheme for smart phone and web, 2015 International Conference on Information Processing (ICIP) Dec 16-19, 2015.

[4] R.Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Computer Surveys, vol. 44, no. 4, 2014.

[5]B. B. Zhu et al., “Attacks and design of image recognition CAPTCHAs,” in Proc. ACM CCS, 2010.

[6]Design and Implementation of Password-based Identity Authentication System-2010 International Conference on Computer Application and System Modeling (ICCASM 2010).

[7] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on pass points-style graphical passwords,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, Sep. 2010.

[8] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in Proc. ESORICS, 2007.