A Review On CAPTCHA as Graphical Password – A New Password Scheme

Yogesh Pandey[1],Amol Saxena[2]

[1]*Department of Information Technology, Poornima College Of Engineering, Jaipur,*
[2]*Assistant Professor, Department of Information Technology, Poornima College Of Engineering, Jaipur.*

[1]*2014pceityogesh060@poornima.org,*[2] *amolsaxena@poornima.org*

Abstract

This review paper is aimed at studying the present password system and then analyzing it and implement a new password system. CaRP uses CAPTCHA and graphical password to solve a number of security problems. In CaRP user is allowed to set his/her password using a combination of captcha and graphical password scheme.Every time user login to the system a new captcha challenge is introduced to the user and user has to derive his/her password out of that captcha puzzle. Captcha is a challenge that only humans can pass. So it is impossible for computer program to pass the puzzle resulting in more security. CaRP is more user friendly as it uses graphical password scheme making password more interesting for users.

Keywords: *new password scheme, CaRP, secure password*

1. INTRODUCTION

There are many problems in User authentication. And for authentication purpose computer security depends on password. Password has some important characteristics which are as follows:

1. It should be changeable.
2. It should be quickly and easily executable.
3. It should be easy to remember.

Authentication is must and is an important step for accessing any system and we generally use text password as a security technique but these are threatened by attacks and are not safe. These can be hacked and can be attacked by phishing, brute force attack; dictionary attack etc. among this phishing is a serious threat to text based password.

Through phishing one can get information such as user details like username, password, and contact information And other details by masquerading attack.

The challenge with text password method is difficulty in remembering them. To solve the problems with old username and password authentication system, an alternative authentication scheme such as Graphical password is a solution. Humans are more likely to recall pictures and line drawing object or real objects than texts so we can set graphical password as the password scheme. So this will remove the big challenges.

In Graphical password images can be set as password thus resulting in easy recalling of password and this scheme of password implementation is more user friendly then conventional password scheme to text password.

In addition to web login application and work-stations, graphical passwords have also been used to ATM machines and mobile devices so this password scheme can be implemented to all these places.

The biggest problem with old password scheme was that computer programs were generated to crack the password and password was breakable through many computer attacks. CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is programs that generate tests that are human solvable, which can't be guessed through current computer programs. Hence in solving captcha human involvement is must. Defending the sites against various attacks such as bots, resisting automatic adversarial attacks is possible through the program of implementing Captcha.

Captcha also prevents system from dictionary attacks, spam and worms. CaRP is Captcha as a graphical

password, which is a combination of both captcha and graphical password as a single entity for authentication. IN CaRP click-based graphical password strategy is implied. It differs from other password scheme as in graphical password scheme only one image is used and user has to click on that image for authentication but in CaRP images used are Captcha challenge for the user, and for every login attempt a new CaRP image is generated. CaRP solves a number of security problem altogether that are online guessing attacks, relay attacks etc. and, if combination with dual-view technologies like graphical password or text password it can minimize shoulder-surfing attacks. In this review a difference has been studied between existing password scheme and CaRP technology.

2. Graphical Passwords

There are several graphical password methods. Recognition, recall and cued recall these are the three methods of graphical password system and these ivolve the of memorizing and recognizing the password involved. In recent review more methods can be found. A recognition based technique requires identifying the objects from a set of given objects that belongs to the password which had been already defined by the user. The scheme is Pass faces in which a user creates password by choosing a set of faces from a Database. In authentication, user selects a face belonging to her portfolio from a panel of faces represented to her. This method is repeated many times, each time containing a different set of faces.

In each round the image set remains the same but the images are permuted randomly. Correct Selection in each round leads to successful login. An extra hint is provided to user in cued-recall technique, so that user can easily memorize and enter the password. In this scheme users are required to memorize the specific points present in image. PassPoints is click-based cued-recall scheme in which a user picks particular points at anyplace on an image by clicking on them thus creating a password and user must click on those points while authenticating. Deterministic function to select next images and one click per images as in Pass Point are used by Cued Click Points (CCP). Among the three types recall is the hardest for users (human) memory while recognition is easiest to remember.Recognition is also the weakest in resisting guessing attacks.

3. Captch

Captcha are the challenges that can be solved by humans only as captcha asks general question or give problems which are very easy for humans to answer but almost impossible for computers to solve as they need to identify the objects and then apply algorithm, but each time a new random captcha gets generated resulting in failure of predefined program to solve captcah.

Captcha are of two types: Text Captcha and Image-Recognition Captcha.

The Image Recognition Captcha is based on recognition of non-character objects and text Captcha depends on character recognition. The characters in text captcha are generated randomly and are human readable but difficult for computer to answer as these are represented in different fashion than usual.Non-character object recognition by machine is more difficult and complicated as compared to character recognition thus making IRCs more secure than text Captcha. In Asirra the binary object classification is done in which user is presented with a set of images with some images possessing some similarities and user is asked to click all the images having some common property. Thus this kind of challenges can be solved by humans only because of the fact that computers are not capable of finding similar objects because each time a different set is introduced as a challeng.

4. CARP

An Overview: In CaRP, a new image is generated each time the user tries a login attempt. CaRP generates the Captcha challenge by using the alphabets of visul objects like alphabets, numbers, characters and similar objects. The main difference between both the schemes is that in CaRP is that the password is derived from the images presented to user but in Captcha user has to answer some general question or has to write some text or symbols. CaRP uses the click-base technique of graphical password. The CaRP scheme has two types for setting up password which are: recognition and recognition-recall. These techniques requires recognition of the objects which have been settled as password and using these objects as clues at the time of authentication.In Recognition a user is presented with a set of images and user passes the authentication by identifying images that had been selected during registration.In Recognition-recall an extra cue is provided to user to remember and enter the password.

5. METHODS AND MATERIALS

5.1 Captcha Authentication

CAPTCHA means Computer Automated Public Turing Test to tell Humans and robots Apart.

Captcha authentication is normally used to detect bot attacks as bots are unable to type the characters or number in the Captcha. Captcha can be further classified as:

1. Click Text
2. Captcha Animal
3. Animal Grid

Using Captcha makes it difficult to detect the password and also prevents machines/programs to send messages or access accounts without human involvement thus providing more security and authentication.

5.2 Converting Captcha To Car

In principle, any pictorial Captcha scheme depending on classifying two or more predefined type of objects can be transformed to a CaRP. Mostly all the text Captchas and Image Recognition Captcha meets this requirement.

The IRCs can be converted to CaRP by adding more images to it and make CaRP more difficult to solve.

In observe, conversion of a particular captcha theme to a Carp generally needs a case by case study, so as to make sure each security and usefulness.

Some IRCs depends on recognizing objects whose kinds are not predefined. A typical example is Cortcha which relies on context-based object acknowledgment wherein the object to be predict can be of any type. These IRCs cannot be transformed into CaRP since a set of pre-defined object types is vital for building a password.

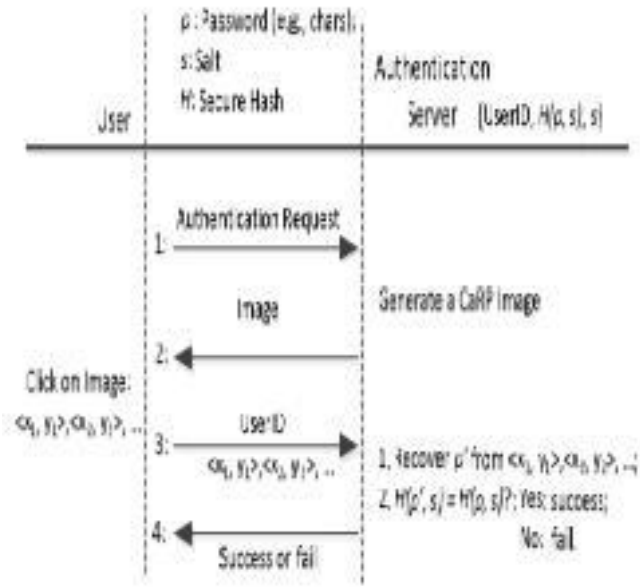

Fig. 1. Flowchart of basic CaRP authentication.

1. Click Text:

In this user sets password at registration time and is asked to regenerate the password by presenting an image that contains a set of letters and special characters.

2. Animal Grid:

In this scheme user sets password as a sequence of animals by clicking on animal images. The user is presented with an image containing animals and user has to withdraw the same sequence of animals as stored at the time of password generation, and if both the password matches each other than the authentication becomes successful. For animal images animal image dataset is used. In which multiple small sized animal images were present.

3. TextPoints4CR:

In this method user sets password by clicking on defined points of a large character and at the time of authentication the coordinates are checked and if the coordinates match than authentication becomes successful.

4. Shuffle Text:

This method is same as Click Text method but the only difference is that user can enter password in any manner like in reverse order, shuffled order.

6. IMPLEMENTATION

This CaRP technology can be used for authentication of user on any system or on any interface through registration in which user sets the password and then login process in which user authentication is done.

The Basic system flow is as follows:

6.1. Registration process:

Step1: User selects any CaRP system for registration and authentication purpose.
Step2: The very first step is to select the registration option and enter the basic details and then user selects any of the CaRP scheme recognition or recognition-recall and for security, user answers to secret security question and finalize password.
Step3: Finally user registers. After successful registration user details are stored on a web server and selected scheme is applied as part of security
.

6.2. Login process:

Step 1: User selects an activity for the purpose of login.
Step 2: Login screen is open and user will see a panel in which he/she has to enter the password.
Step 3: User follows the login procedure with respect to CaRP scheme which has been selected at the time of registration.
Step 4: If user passes the CaRP challenge than can access the system ,else user will get redirected to login screen again. If user crosses the maximum no of login attempt than will be asked to answer the security question for further process otherwise the user will get blocked.
Other implementation is that this CaRP scheme can be set as secondary password scheme for user for the security purpose of confidential data. If by any means someone has access to the system then also setting CaRP as secondary password can save the data from any read/write action or from downloading.

7. CONCLUSION

Reviewed about CaRP, this is a new security method that originated form unsolved hard AI problems. CaRP combines two technologies for making more secure password scheme that is graphical password and Captcha system. CaRP introduces new security levels by providing a new image as challenge to withdraw password for each new login attempt. It also provides security against guessing attacks, brute force attacks and relay attacks. The main advantage is that CaRP doesn't rely on any specific Captcha scheme so if one scheme get broken a new robust scheme can be introduced.

REFERENCES

[1] Ieeexplore.ieee.org. (2018). Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems - IEEE Journals & Magazine. [online] Available at: http://ieeexplore.ieee.org/document/6775249/?reloa d=true [Accessed Mar. 2018].

[2] Anon, (2018). [online] Available at: https://www.researchgate.net/publication/26429217

[3] 6_Captcha_as_Graphical_Passwords-A_New_Security_Primitive_Based_on_Hard_AI_P roblems [Accessed 9 Mar. 2018].