Captcha as Graphical Passwords (CaRP) - A Novel Security Approach Based on Hard AI Problems

S. Manasa¹, C. Rajendra², G. Venumadhava Rao³

¹,² Department of CSE, ASCET, Gudur, AP, India
³ Faculty of Computing, Botho University, Gaborone, Botswana

Abstract- User authentication has become one of the important topics in information security. Many graphical password schemes have been proposed, which are used to improve password usability and security. In this paper, we present a new approach to solve the hard AI problems, namely, graphical passwords are combined with Captcha technique, which will be referred them as Captcha as graphical password otherwise we call it as CaRP. CaRP solves security problems such as online dictionary attacks, relay attacks and shoulder-surfing attacks combined with dual-view technologies. Captcha as graphical passwords also offers an efficient approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass-Points. CaRP also offers primitive scheme to provide reasonable and usability security to improve online security.

Keywords- Password, Captcha, CaRP, Graphical password, Invariant Points, dictionary attack, relay attack, online security.

1. INTRODUCTION

Security is imperative factor in today’s world. Most of the daily activities such as education, searching are dispensed through the web. It is fundamental issue for getting to private information and security parameters. One of the most important fundamental is authentication, to ensure data security issue is that the trouble of recollecting passwords provided by user. Studies have demonstrated that the clients have a tendency to pick short passwords or passwords that are anything but it is difficult to keep in mind. Shockingly, these types of passwords can likewise be effortlessly speculated or broken. A primitive task in security issue is to create cryptography based on hard math problems. A new exciting primitive (or) novel approach was invented to solve hard AI (Artificial Intelligence) problems for security is Captcha, which distinguishes human users from computers by providing challenge-response i.e., a puzzle, which is hard to computers but easy for humans to solve puzzle. However, this type primitive succeeded very little when comparing with cryptographic technique. In this paper, we provide novel method that graphical passwords are built on the top of captcha i.e., referred as Captcha as gRaphical Password (CaRP). CaRP is click-based graphical password. A sequence of clicks on an image is used to derive a secret. The images are used for the construction of CaRP. A new Captcha based graphical password image is generated for user every login attempt process into the account. The notion of CaRP is straight forward and unique technique, however generic. CaRP will have multiple instantiations. In theory, any Captcha theme relying on multiple object classification will be converted in to a CaRP image. We can present CaRP in two methods, which can be designed on both text based Captcha and image-recognition based captcha. One among them is text-based CaRP, whereby a secret could be a sequence of characters like a text secret, however entered by clicking the proper character at login in a sequence on CaRP images. CaRP provides the security against the online dictionary attacks. A dictionary attack is a type of brute force attack where the attacker uses a dictionary names or any of common text. In the text-based password, dictionary attack creates a dictionary of memorable words such as birthdates,
favorite foods, pet names, or person names as potential passwords. To attack click based graphical authentication, the attacker creates a program that can spot the popular click points on the image. When a dictionary has been created, the attacker can use a program to crack a user login page by trying passwords from the dictionary. CaRP also provides security against relay attacks. Relay attacks are nothing but type of hacking technique related to man-in-the-middle attack. CaRP is secure against shoulder-surfing attacks by using dual-view technologies. CaRP mainly can be applied for online services such as online banking services, email services to avoid spam emails, for legal services etc., because the user requires solving a Captcha challenge for every login attempt.

2. LITERATURE SURVEY

2.1 Overview of Graphical Passwords

The term “PASSWORD” commonly refers to secret used for authentication [5]. Passwords are the most commonly used method for identifying users in computer and communication systems. During 1999, graphical password schemes have been proposed, motivated by providing and improving password memorability and usability, while at the same time improving strength and online security against guessing attacks, relay attacks and dictionary attacks. As like of text passwords, graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret which is in the form text as their password. This method has been shown to have some drawbacks. For example, users are used to take any passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard for user to remember (or) if a password is easy, then unknown user is easy to track [3]. Graphical password schemes can be grouped into three general techniques of passwords: Recognition-based, Recall-based and Cued-recall.

A Recognition-based technique, Dhamija and Perrig proposed a graphical authentication method based on the Hash Visualization technique [2][7]. In this method, the user is asked to select a certain number of images from a set or group of random number of images generated and stored in the database. Later, the user will be required to identify those selected images in order to be authenticated. The time taken for this process, however, is longer than the traditional text-based approach. A weakness of this method is that the server needs to store the images of each user. Also, the process of selecting a set of images from the image database can be time consuming for the user. Akula and Devisetty’s algorithm is similar to the technique proposed by Dhamija and Perrig [6]. The difference is that, which produces an output and occupies less space, the authentication is secure and require less memory.

Weinshall and Kirkpatrick has proposed several authentication schemes, such as image recognition, object recognition, and pseudo code word recognition, and conducted a number of tests on those methods. In the image recognition study, a user is required to recognize a large set of images (group of images) selected from a database. This is the way which showed that image is the most effective among the three schemes tested. Man, et al. proposed another shoulder-surfing resistant algorithm. In this algorithm, user selects a number of images from group of images provided by admin, at each login attempt the form of the images changes. Hong, et al. later improved this approach to allow the user to assign their own codes with different variants such as pass faces [1].

A Recall-based method, Jermyn, et al. proposed a technique, called “Draw- a - secret (DAS)” [4], which allows the user to draw their unique password. A user is asked to draw a simple picture (i.e. any character) on a 2D grid. The coordinates of the grids occupied by the image are stored in server in the order of the
drawing. The user needs to draw his/her password on 2D grid. During login process, the user is asked to redraw the same character on 2D grid. If the drawing touches the same grids in the same sequence, then the users authentication process is success otherwise fails. Jermin, et al. suggested that given reasonable-length passwords in a 2D grid, the password space of DAS is larger than that of the text based password space. Thorpe and van Oorschot extended and analyzed to implement based on the memorable password space of the graphical password scheme by Jermin et al. They introduced the concept of graphical passwords and also observed and studied the possibility of a brute-force attack using such passwords. They defined a length and size parameter for the DAS type graphical passwords and showed that DAS passwords of length 8 or larger on a 2D grid may be less susceptible to dictionary attack than textual passwords. They also showed that the space and memory usage of mirror symmetric graphical passwords is very smaller than the full DAS password space. Persuasive Cued Click-Points (PCCP) is an extension to CCP [9]. The variation of CCP designed to persuade users to select more number of random passwords. It works like CCP, but during password creation the image is dimmed (or) lighting of image changed (i.e. except the clicked position remaining part of the image will be appear like dull) except for a small square viewport area randomly positioned on the particular image. Users select a click-point from within this viewport, or may just keeping the mouse click on the point to select the password and cursor is randomly reposition the viewport until a suitable locations are found. On subsequent logins, images are displayed in their normal format without dimming or viewport. Common wisdom that users choosing the path-of-least-resistance on image means, selecting a click-point within the first or first few viewpoints (viewports).

Using CCP as a base system, we added a persuasive method feature to encourage users to select more secure passwords, and to make it more difficult to user to select passwords. Click-points in CCP are called the hotspots. Users must remember those click-points, if the selected point at login process matched with a click-points at authentication process then login attempt is successful otherwise fails.

2.2 Background work of Captcha

Captcha is referred as Completely Automated Public Turing test to tell Computers and Humans Apart. It also known as Human Interactive Proof (HIP), is an automated Turing test that takes place between the computer and the user in which both generates the challenges and responses (also known as puzzle). AI is nothing but branch of computer science which is referred as creation of machine that works and reacts like humans. Artificial Intelligence Problems which cannot be solved by current computer programs or bots, but are easily solvable by humans. Users who provide a correct response to a challenge that is provided by computer should be guessed and to be solved by human; otherwise it was a bot. Captchas have been widely used as a security measure to avoid the access from bots and unknown users. The most common applications for practical security by Captcha test include online banking, email services, online shopping, different search engine bots, worms and spam, and preventing dictionary attacks. There are two types of Captcha: Text Captcha and Image-Recognition Captcha (IRC).
In a *TextCaptcha*, characters are presented in the form of distorted and connected to prevent from bots. For example, whenever a person needed to create an account (or) to apply any online applications. After filling his/her details there may be presence of text box with group of characters those may be distorted. The user must identify those characters and reenter the characters in empty text box beside the filled text box. Most of the developed or deployed texts Captcha have been broken by the hacker enter into the account as authenticated user. It is possible to enhance the security of an existing text Captcha by systematically adding noise and distortion, and arranging characters more tightly along with some numeric characters. Captchas were originally developed by Vista to avoid the submission of URLs to the search engine. It was a simple Captcha which asks users to type group of characters those are in a distorted English word (or) normal characters. Carnegie Mellon designed the Gimpy method which selects a word from dictionary (or) any random word asks users to type what they see as an image after identifying the distorted image containing the text. Yahoo browser uses the simple version of this method which is called as; EZ-Gimpy. EZ-Gimpy’s image modification and character recognition includes background grids, gradients, non-linear deformations, distortions, and noise in the pixel etc. *Image-recognition Captcha is also called IRC,* Chew and Tygar were among the first to use images (usually images) to create a new method of Captchas, called image Captcha [11]. While several variations of image Captchas exist, image recognition Captchas requires to understand which image is selected as a password on an image which constitutes a hard AI problem. Image recognition Captchas is usually database-based method, thus requiring a database of predetermined images. Microsoft’s Asirra is a well-known example [10]. Asirra presents a list of (or) collection of animal images such as cat and dog etc., images, asking the user to identify the those images and which are entered in the form of characters. In Captcha based Password Authentication (CbPA) protocol used to counter the online dictionary attacks, relay attacks and shoulder-surfing attacks.

3. ACTUAL WORK

The actual work discussed: CaRP Overview in section 3.1. Working and Extensions of CaRP in section 3.2 Recognition-based CaRP in section 3.2.1 Recognition-Recall CaRP in section 3.2.2.

3.1 CaRP Overview

Captcha and Graphical passwords are combined together, which technically referred as “Captcha as graphical password”, that is additionally call it as CaRP (Captcha as gRaphical Passwords). CaRP is click-based graphical passwords, where a sequence of clicks on a CaRP image is used to derive or reveal the secret behind the image. Like other click-based graphical passwords, the main difference is that all the images which are selected at the time of authentication process should be entered in the form of characters that is stored in database of admin. Whenever users are performing the login process the user should memorize the password which is entered at time of logging process. CaRP offers reasonable and usability protection against online dictionary attacks, relay attacks, online guessing attacks and shoulder surfing attacks. In online guessing attacks the unknown user performs ‘n’ number of trails to track or trace the password. The number of trails for password is used for secret guesses that decreases with a lot of n number of trials are used. Mathematically, let S be the set of secret guesses before any no. trial, ρ set of password, T denote a trial where as $T_n$ denote the n-th trial, and ρ (T = ρ) be the chance that ρ is tested in trial T. Let $E_n$ be the set of secret guesses tested in trials up to (including) $T_n$. The password guess to be tested in n-th trial of $T_n$ is from set of $S\setminus E_{n-1}$ then,
\( \rho(T = \rho | T_1 \neq \ldots, T_{n-1} \neq \rho) > \rho(T = \rho) , \)

And \( E_n \to S \)

\( \rho(T = \rho | T_1 \neq \ldots, T_{n-1} \neq \rho) \to 1 \) With \( n \to |S| \)

\(|S| \) defines the cardinality. Each trail specifies tested password is actual password or not within \(|S|\) trails. This approach is used to guess guessing attacks which can be avoid by CaRP scheme. CaRP based on graphical passwords can be classified into two methods: Recognition CaRP and Recognition recall based CaRP method.

3.2 Working and Extensions of CaRP

3.2.1 Recognition CaRP Scheme

In this type of CaRP scheme, a sequence of visual objects is stored in form of alphabets. Recognition CaRP looks to access infinite range of various visual objects. ClickText method, ClickAnimal method, AnimalGrid method are three types are present in Recognition CaRP. In ClickText, characters are arranged randomly on 2D grid space which is provided by server. The characters are ordered from left to right, the user should select some characters as a password. For example, user selects \( \rho = "QUBIC" \), the user should remember this password for every login attempt. In the same way ClickAnimal, there may be presence of different animals user should select animal and enter with alphabets such as \( \rho = "cat,dog,lion..........." \). Another type of technique which is used in Recognition based CaRP is AnimalGrid method; user is needed to enter a password. ClickAnimal image is obtained first. After selecting the animal, an image of grid-cell appears with numbers which are not in order. Therefore a password is sequence of animals and grid-cells. For example, user selects \( \rho = "fish(3),dog(5)........" \). The Recognition CaRP was implemented by using Dhamija and perrig algorithm. Hash values are generated for every user. Hash values are used to access the data for security. It is also called as message digest, a number is generated from string of text. The flowchart of basic Recognition CaRP shown below:

![Flowchart of basic Recognition CaRP](image)

The authentication server (AS) stores a salt \( S \) and a hash values \( H \) for password generated as \( H(\rho, s) \) at authentication process, where \( \rho \) is password and \( s \) is salt value. Upon receiving a login request, AS generates a CaRP image, records the locations of the objects within the image, and sends the image to the user to click her password. The coordinates of the clicked point's area unit recorded and sent to AS together with the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects \( \rho' \). Then AS retrieves salt \( s \) of the account is retrieved, calculates the hash values of \( \rho' \) with the salt, and compares the result with the hash value hold at authentication. Authentication succeeds as long as the 2 hash values match. In server, password stored along with salt value (i.e., random value taken by user) and hash value is generated as \( H(\rho, s) \). At every login attempt of user server generates hash value as \( H(\rho', s) \). If hash values of authentication and login process matches, then login attempt is success otherwise fails. For example “word” is
password selected by user as CaRP. The password stores with formula in server as:

\[ S_0 \times 31^{(n-1)} + S_1 \times 31^{(n-2)} + \ldots + S (n-1) \ldots (1) \]

The value of password “word” (i.e., 72 possible characters are 26 uppercase, 26 lowercase, 10 numbers, 10 special characters). Calculating the “word” with the above formula i.e., some 1138. Server selects some random value as salt values suppose 4. Server generates hash value with formula \( H(\rho, S) = \rho \mod 2^s \). The result will be stored in server as 71.1(appox). Whenever user performs login attempt the hash value should be equal to value generated at authentication process.

3.2.2 Recognition-Recall CaRP Scheme

Recognition recall CaRP scheme is a sequence of some invariant points of objects. Invariant points are nothing but some collection of points is selected on a particular image at the time of authentication process. User should determine the objects during a CaRP image creation at the time of authentication, so use the known objects as cues or the password to find and click on particular image clicking on the invariant points.

Recognition-recall CaRP scheme classified into two types: TextPoints and TextPoints4CR. TextPoints looks different to ClickText; they are generated in similar way except clicking on the locations. Invariant points are also called clickable points. This is nothing but internal points of the selected character by user from server. Each character contains large number of different invariant points. TextPoints are nothing but, a collection or a set of internal invariant points of characters is selected to form a set of clickable points. To determine clickable points, the distance between any two points or pair of invariant points or clickable points must not exceed the threshold value such that no invariant point overlaps with another invariant point. The minimum distance between any pair of points should be larger than \( \mu \) by that margin which exceeds a threshold to prevent two points falling into same grid-cell point.

A sequence of clickable points is applied to character which is selected by user at time of authentication process which was sent by server. TextPoints occupies more password space and memory in server. Recognition recall CaRP scheme was mainly implemented by using Blonder algorithm. Later Wiedenbeck et al. extended Blonder’s idea, wherein the authentication server no needs to store the hash value and salt value. The server provides the particular image at the time of authentication process. The user must click on the different locations of a particular image. The image of Recognition- recall scheme shown below:

![Recognition-recall CaRP Image](image)

In this scheme, for comparison purpose entropy comparison is required. For example size of the image is \( \mu \), \( \tau \) number of locations to be selected on image. The distance between the two points should be less than 0.5\( \mu - \tau \). In which these locations are stored in the form of coordinates (i.e., x-coordinates and y-coordinates). At the authentication process, server sends the image to the user. User should select
different locations on particular image the distance must be less than $0.5\mu - \tau$. The selected points are stored as the password. Every login attempt of the user, server compares the user entered password and authentication password by using entropy formula i.e., $n \times \log_2(30)$, where ‘n’ represents number of locations and 30 represent the salient points. If both the values matches then login attempt is success.

4. CONCLUSION

CARP is collection (or) a combination of both Captcha and graphical password is a new technique introduced to protect the online services against the dictionary attacks, relay attacks, and online guessing attacks which we referred as hard AI problems. CaRP is combined with dual-view technology to avoid shoulder surfing attacks. At every login attempt of the user a new CaRP image or CaRP text is created. Our implementation is one step forward by combining Captcha and graphical password. In future CaRP can be extended by using DAS method.

5. REFERENCE


