

# Captcha as a Graphical Password

Kashmira Bagul<sup>1</sup>, Ashwini Bhalerao<sup>2</sup>, Pratiksha Godge<sup>3</sup>, Shweta Kale<sup>4</sup>

<sup>1</sup>Student, Information Technology, MET BKC IOE, Maharashtra, India

<sup>2</sup>Student, Information Technology, MET BKC IOE, Maharashtra, India

<sup>3</sup>Student, Information Technology, MET BKC IOE, Maharashtra, India

<sup>4</sup>Student, Information Technology, MET BKC IOE, Maharashtra, India

## ABSTRACT

Hard mathematical problems are used by many security primitives. In this paper, we present a new security primitives as file stored in as network using Captcha technology, which we call captcha as a graphical password (CaRP). CaRP is a graphical password scheme and also a captcha. CaRP solve various security problems such as online guessing attacks, shoulder-suffering attacks etc. Even if the password is in the search set, a CaRP password can be found only probabilistically by automatic online guessing attack. Captcha is now a criterion Internet security method to define online email & other services from creaturebatered by bots. CaRP offers reasonable security & usability which fit and well some practical application for improving online security CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

**Keyword :** - Graphical password, CaRP, CCP, security primitives, CAPTCHA.

## 1. Introduction

Nowadays internet acts as an important role. Every person will browse to get their respective necessities. Internet is useful in many different ways. Everyone desires to browse securely that is they need their personal things to be ensured like passwords or any text file. As the use of internet develops the hackers are also born, i.e. user's personal documents or passwords are hacked by the third person usually called hackers. As use of internet is important likewise protecting our personals is also an important thing. Here mean to say that there should be an implementation of security for the user's personal documents. The use of authentication mechanisms can also prevent authorized users from accessing information that they are not authorized to view.

Usable and cost effective user authentication mechanisms to help mainly the computer users those are working on untrustworthy computers, Internet, and unsafe networks. This project proposes a Cued Click Points (CCP) for graphical password authentication. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security.

A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. The user should click on that image or on any part of that image as a password and that image or clicked particular part will be stored as their graphical password and those images are differently generated for different users.

A user can login to their websites by entering their username on the browser and typing their password on to their cell phones which would be converted to a one time password. And to provide a more secure system this provides encryption for the converted one time password. So a more secure user authentication system is introduced in which, the user only have to remember a click points. Hence introduce a security for the users so they can browse safely and their personals will be safe.

In the few years ago the network security is the most important things. Some used as a in simple way that is password the password .the password are easy to use and easy to hacked so we are introducing the new security primitives that are based on mathematical problems. The cryptographic primitives based on hard math problems and their wide applications. And the hard AI problem are used for the security is emerging as an existing new typical example. we are presenting a new security primitive that are mostly based on hard AI problem, which are more friendly of the most top of captcha technology.

the security is to create cryptographic primitives based on hard mathematics problems that are computationally intractable by using fundamental task. Using artificial intelligence hard problem for the security it is an exciting new typical example.

The best example is puzzle it friendly with computers but its is easy for the humans. Captcha standard is the technique to protect online email and other service from abused by bots ,Hence that we are called as CARP the CaRP stand as the captcha as graphical password. CaRP is click-based graphical password, where it is a sequence of click on an the image is used to the a drive a password .The unlike other click based graphical passwords, image which mostly used in CaRP are captcha challenges and a new CaRP image is generated for every logic attempt. CaRP is the notation is simple generic its have multiple instantiations. Captcha scheme relying on ,multiple-object classification can be converted a CaRP scheme. CaRP is a scheme that are both a captcha and as graphical CaRP has a many number of address security problem almost that such as online guessing attacks, relay attacks and its combined with dual-view technology and the shoulder suffering attacks. CaRP is the password that can be probabilistically found by the automatic online guessing attacks so the pass so it should be in the search set.

## 2. Literature Survey

**2.1 Graphical Passwords** A richly number of graphical password systems has been suggested. They can be classified into three categories allowing to the task needed in memorizing and coming in passwords: identification, recall, and cued recall.

- 1) Recognition-based scheme
- 2) Recall-based scheme
- 3) Cued-Recall based scheme

A recognition-based scheme demands discovering among decoys the visual objectives belonging to a password function. A distinctive scheme is Pass faces where a user chooses a function of faces from a database in giving rise a password. During certification, a panel of candidate faces is showed for the user to select the face going to her function.

This process is iterated various attacks, each round with a different board. A successful login calls for correct selection in each round. The band of images in a panel stays the same between logins, but their positions are permuted. Story is similar to pass faces but the images in the function are governed, and a user must key out her function images in the discipline order.

A recall-based scheme calls for a customer to regenerate the identical interaction result without cueing. In recall-based, without any clue or hint user generate his password. It follows many algorithms, which include passdoodle, DAS (draw-a-secret) and many more.



**Fig -1 Passdoodle Scheme**

Recognition inhibits the common use of the Passdoodle. Length and identifiable features of the doodle provides the boundaries of the system. A distinct number of computer differentiable doodles are possible. The doodle here is used as the only means of identification. A basic floor threshold of likeliness and similarity 11 for reasons of security, must be set, seeing as the system would refuse to authenticate a user as the user whose recorded doodle is most similar. This prevents guessing to authenticate a random user.

In Cued-Recall based scheme, the image cues the user. For eg. to click a set of option a set of point on an image means hint and reminder help user to reproduce their passwords. It follows many algorithms, which include pass points, CCP (cued click points), PCCP (Persuasive cued click points).

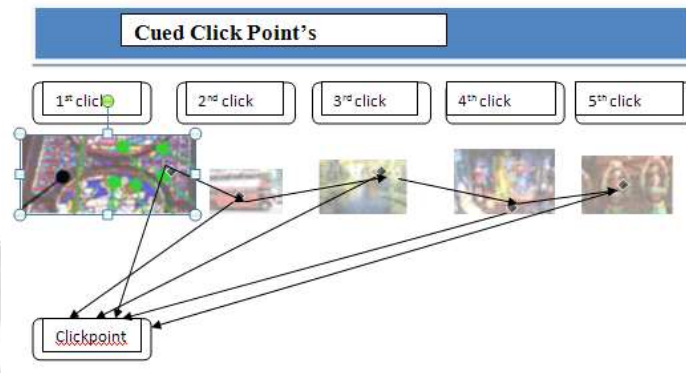


Fig -2 CCP

Cued Click-Points (CCP) is a click-based scheme where users select one click-point on each of 5 images presented in sequence, one at a time; this provides one-to-one cueing. The next image displayed is depend on previous image location (i.e. where the user click on previous image). Users gets immediate feedback if they click on wrong location during login, seeing an image that they do not recognize. At this point they can restart password entry to correct the error. This feedback is not useful to a hacker not knowing sequence of images.

**2.2 Captcha** Captcha trusts on the gap of capacities between individuals and bots. There are two forms of picture Captcha: text Captcha and Image-Recognition Captcha (IRC). The previous relies on character recognition while the second relies on identification of non-character objects. Protection of text Captchas has been extensively read. The following principle has been launched: text Captcha had better rely on the struggle of character partitioning, which is computationally pricy and combinatorial tough. The example of captcha is shown in Fig-3

Fig -3 Examples of captcha



**2.3 Other Concerned Work** Captcha is utilized to assist delicate customer inputs on an untrusted client. This scheme shelters the communication channel between customer and Net server from key loggers and spyware, while CaRP is a family of graphical password systems for user authentication

### 3. Proposed System

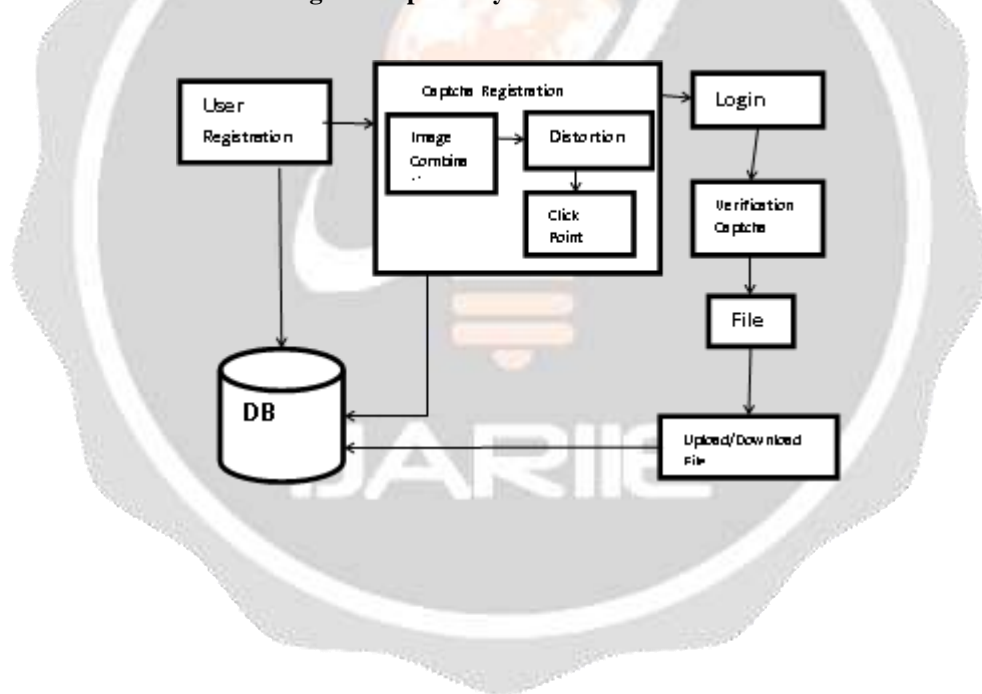
In our system designed follows the 3 phases for securing your data. This three modules which is developed by us: user registration module, pictures selections module and last system login module also a file upload needs the security second picture selection module is used after login also.

Design Module:

1. In user registration module traditional way of registering a user is done. This user's data is stored in the database a dosed during the login phase for verification.
2. In picture selections module firstly we take user picture for login of that user. User will click on that picture of his/her then the Captcha will be viewed for the user. In the registration we will select any image as password and consist of a sequence of five. Click-points of a given image. User may select any pixels in the image as click points for theirs password. User needs to select a click-point in the image & proceed on the next five images.
3. During login process the user picture will be displayed user checks the picture and selects it and proceed & then sequence of clicks in the correct order should be clicked in registration phase.

An important usability goal is that to help user's select better password with larger password space. By using cued click point provides great security using hotspot technique. In addition to offering protection from online guessing attacks. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then analyze for hotspot on each of these images. Using CCP advantage is that it increase the authentication, memorable, security and usability is simple.

**Fig -4 Proposed System Architecture.**



The above diagram shows the architecture of proposed system, in which database is connected with the captcha registration and also upload and download file field used by users to store the documents such user can store important details of the user such passwords, files of the organization, various documents of industry etc. In Captcha Registration combinations of images are showed sequentially and that sequential images are in distorted forms and user needs to click on image with five different points. This click points are saved in database for user login. In each image there is a one question asked to the user and user needs to select the point by giving the answer such as if the first image contain the question where is dog? After that user clicks on dog and that click point will saved in the database for further login process. In this way user captcha registration is done. In the login attempt database check for authorized user if this user is authorized user or not by checking the sequence of click points. Here time taken for the clicks are less so this is efficient to use and attacker needs time to guess the password so attacks on the system is less. In file uploading and downloading, sequence of images are showed for securing the data of user which has been stored in database. This new feature for file store system is introduced in our system using captcha password for uploading/downloading. We are using Cued Click Point (CCP) algorithm for sequencing of images and also the



clicks. Cued Click Points (CCP) is like Pass Points but utilizes single picture per click, with the following picture took by a settled work. Persuasive Cued Click Points (PCCP) stretches CCP by needing a user to pick out a point inside a randomly placed viewport when creating a password, leading in more at random spread click-points in a password.

**Fig -5 Captcha will look like this**

*CaRP:*

CaRP is a family of graphical password systems created with Captcha technology. Just like PassPoints, a user clicks on a CaRP image and the sequence of her clicks creates a password. However, each CaRP image is automatically generated by a Captcha generator, and thus is also a Captcha challenge. Just like a session key, a CaRP image is never reused across different sessions. Even for the same user, a new CaRP image is needed for every login attempt. To the contrary, in PassPoints a user always uses the same image to click her password, and many users use the same image for their password input, which leads to successful attacks exploiting hotspots. The notion of CaRP is simple but generic, and it can have multiple instantiations. Many Captcha schemes, regardless of whether they are text based or image recognition based, can be converted to a CaRP scheme.

The hardware and software specification for project:

Hardware Specification: Speed up to 1.1 GHz, RAM -256 MB (min), Hard Disk 20 GB (min), Floppy Drive -1.44 MB

Software Specification: Operating System Windows95/98/2000/XP, Application Server Tomcat5.0/6.X, Front End is in HTML, Java, Jsp, Scripts JavaScript., Server side Scripting is done by Java Server Pages. Database is MySQL 5.0, Database Connectivity is done by JDBC.

#### **4. Conclusion**

The Cued Click-Point method is very usable and provides great security using hotspot technique. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image. Cued Click Point is more secure than the previous graphical authentication methods. CCP increases the workload for

attackers by forcing them to first acquire image sets for each user, and then analyze for hotspot on each of these images. Cued Click-Points method has advantages over other password schemes in terms of usability, security and memorable authentication mechanism.

## 5. References

- [1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords- A New Security Primitive based on hard AI Problems" Proc IEEE VOL.9,NO.6,June 2014
- [2] Mekha Mariyam Thomas, "Secured Paasword Technique Using Devices"VOL.16, NO.8, Sep-Oct 2014
- [3] Rashmi B, B Maheshwarappa, "Improved Security using Captcha As Graphical Password"VOL.4,NO.5,May 2015
- [4] U.Anitha , S.Shakila , V.Kavitha" Implementing Captcha as Graphical Passwords Based on Hard AI problems"VOL.1,NO.9, March 2015
- [5] Navgire Priyanka D, Jayapal PC, Kulkarni Swapnali V, "Graphically Secured Password"VOL.2, NO.11, Nov 2014
- [6]Vaibhav Morasakar, Sagar Jaikalyani,Muib Sayyed, Jaykumar Gurani, Kalyani Pendke"Cued Click Point Technique for Graphical password Authentication"VOL.3,NO.1,Jan 2014

