A SURVEY ON VARIOUS CARP TECHNIQUES

Mihir Chakradeo[1], Mohit Khatwani[2] ,Akshay Munde[3] and Abhishek Oswal[4]

Abstract: Captcha as a Graphical Password is a technique which is a combination of Captcha as well as a graphical password scheme. It enables us to address a plethora of security problems in an unprecedented manner such as brute-force attacks, relay attacks, shoulder surfing, phishing, etc. It is not only a novel means of avoiding the aforementioned, but also makes sure that the users select strong passwords that too in a dynamic manner. The following paper reviews different techniques currently being used under this paradigm, and also proposes a new method with the added functionality of machine learning.

Keywords: Security, CAPTCHA, Machine Learning , Graphical Passwords, Captcha, CaRP.

INTRODUCTION

With the advent of computers and information age, computer security has become a critical part of today's world. The main aim is to provide a system infused with cryptography which makes it difficult for any attackers to gain access to the system or data. With different paradigms of security available today, the most common one, which is the text based password is totally dependent on the length, complexity, and the unpredictability of the passwords. However, as humans, we tend to select passwords which are easier to remember, and thereby compromising the complexity, which in turn leads to easy cracking of such passwords.

CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) has been a commonly used technique for web security against spam bots. The basic principle is to devoid access to robots by differentiating them from actual human users. It involves interactive puzzles or problems which can be specifically performed only by a human. Comment Spam Prevention, Online Polls, Search Engine Bots, Free Email Service, etc. are some of various applications of CARP. There are various methods for deploying captchas, most common of which involve scrambled text, graphical image selection, audio based, video based, etc. This paper covers a paradigm for security using the graphical captcha technique.

A new security primitive based on graphical passwords and captcha (CaRP) is a click based password scheme in which the user is prompted with some interactive objects to click, that too in a proper sequence, to generate a unique password or authentication. The beauty of these schemes is that, the difficulty can be easily increased by increasing the complexity of the image. Not only does it secure against bots, but also against shoulder surfing attacks.

The paper covers various topics like Text Based Captcha Scheme, Graphical Based Scheme, Video Based Scheme. The paper will then propose an improved scheme based machine learning. Lastly, the paper will conclude with the comparison of the aforementioned.

TEXT BASED PSSWORD METHODOLOGY

Basically there are three types of graphical password schemes, that is recognition based system, Pure Recall based systems, Cued Recall based system. As shown in the figure 1 shows the segregation of the techniques.

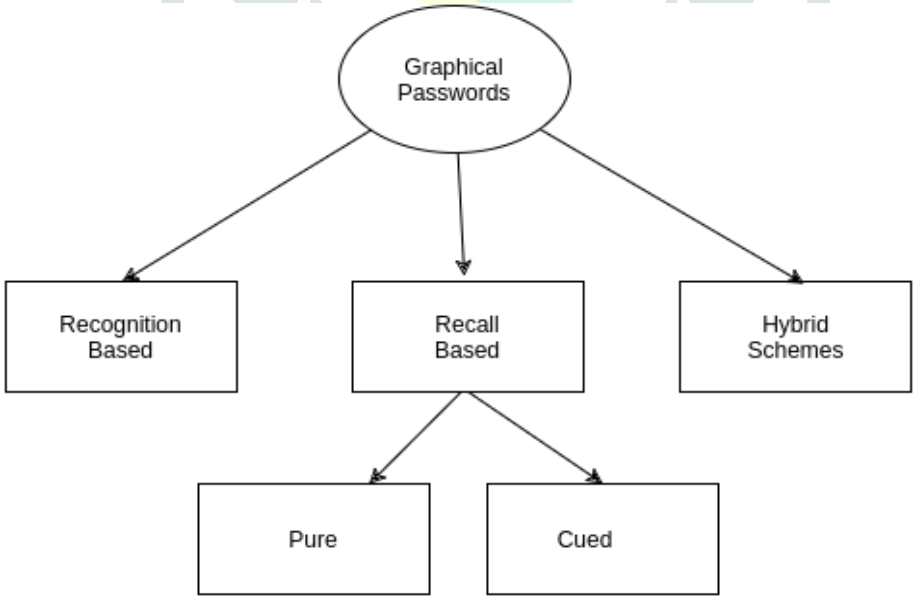

Fig 1: Graphical Password Schemes

RECOGNITION BASED SYSTEM

In recognition based system, the user has to upload a set of images, symbols while registering for the first time. Afterwards when the user wishes to log in, in order to authenticate he has to identify the set of images, symbols which have been uploaded by him among a larger set of symbols and/or images.

S. No.	Scheme	Description
1	Cued Recall	In this system a framework of gestures, hint and reminders are proposed which make it easier for the user to reproduce the password
2	Recall Based	In this system the user has to reproduce something which he had selected or created earlier during the registration phase
3	Hybrid Scheme	This is basically a combination of two or more schemes. For example, textual and graphical password schemes or a combination of recognition and recall based schemes. While alphanumeric passwords rely on a single stage many graphical passwords systems require the user to pass a number of stages or challenges to authenticate

Table 1. Shows classification of recognition systems

VIDEO BASED PASSWORD METHODOLOGY

The CaRP scheme with Video-Based Captcha is enhancing the Captcha schemes with motion through video embedding technology. The Captcha is provided with random motion to objects in Captcha changing background texture, changes in position, angle, shape, size and color in the window, size, providing user with random set of code word in dynamic manner to overcome the attacks using Image-processing or vision techniques [2]. This can be applied to different CaRP schemes like AnimalGrid, ClickText and ClickAnimal. During registration process the characters in code word are first set and then they are embedded in the video creating motion on CaRP scheme. so that user feel that the objects are moving smoothly. Fig 3 shows an animated Captcha with a moving background.

ARCHITECTURE OF CLICK BASED SCHEME

This system involves selecting a random object from the image. The different capture check-points are generated based on the user's clicks. Depending on the nearest checkpoints, hash values are calculated at server side . These hash values are nothing but a function H (p, s) , where p is the password, and is the corresponding hash value. The hashing techniques provides the advantage of not having to store the passwords in the database, thus making it more secure. On clicking the image, the hashing values generated at runtime are matched with the already existing hashing values in the database for authentication [1]. Figure 2 [1] shows the flowchart for the authentication technique.

Fig 2: Authentication Flow Control [1]

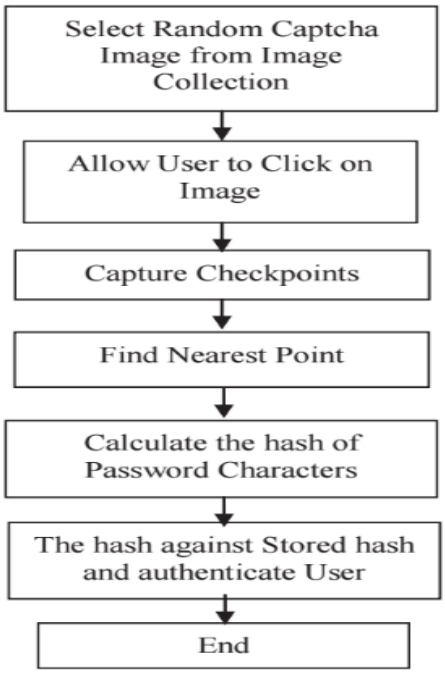

Fig 3: Animated Captcha Example [2]

OUTCOME

The major task for a bot is to identify the characters or objects present in the animated screen The dynamic motion creates difficulty in predicting the movement so provides more security.

The attacker with the idea of tracking or predicting the motion by analyzing the coordinates cannot retrieve any information regarding the object as all the objects are moving hence it is difficult and time consuming to separate background and moving objects. This technique can overcome the static OCR attacks. As the objects are in random motion so a bot finds it difficult to solve it and detect the motion.

CaRP embedded with motion is resistant against dictionary attack, online guessing attack, etc. and provides high robustness to identify higher level challenge used. So the proposed scheme can offer resistance to many attacks and ensure higher level security for a security-based system

PROPOSED TECHNIQUE

CaRP technology uses click-based graphical passwords, where a sequence of images is clicked to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

Step1: Registering : the machine learns the user's mathematical ability based on a test, and assigns a particular function as a password.

Step 2: Mathematical function is assigned based on an adaptive test which judges the ability of user based on number of questions attempted correctly.

Step 3: On login attempt, an image prompt shows up, which has randomly generated numbers.

Step 4: The user then selects the number by clicking on the image, and applies the designated mathematical function to that number, which becomes the password for that session.

Following are the Data Flow Diagrams which give an overview of the flow of the system.

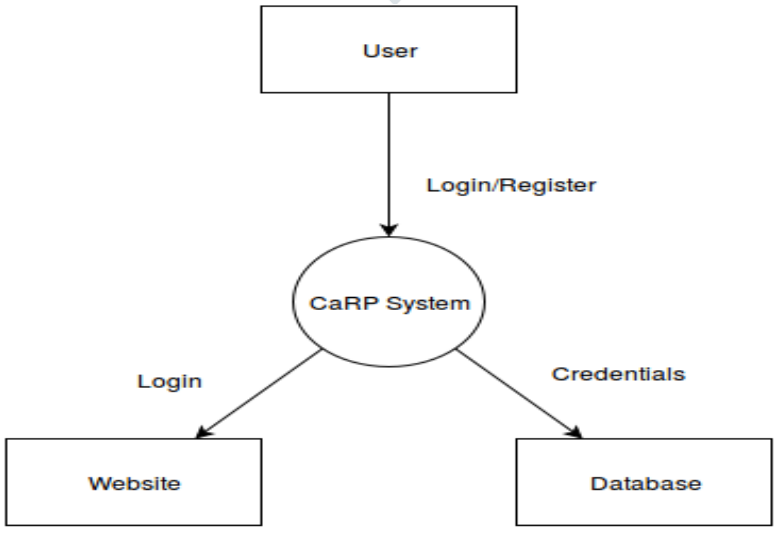

Fig 4: DFD Level 0

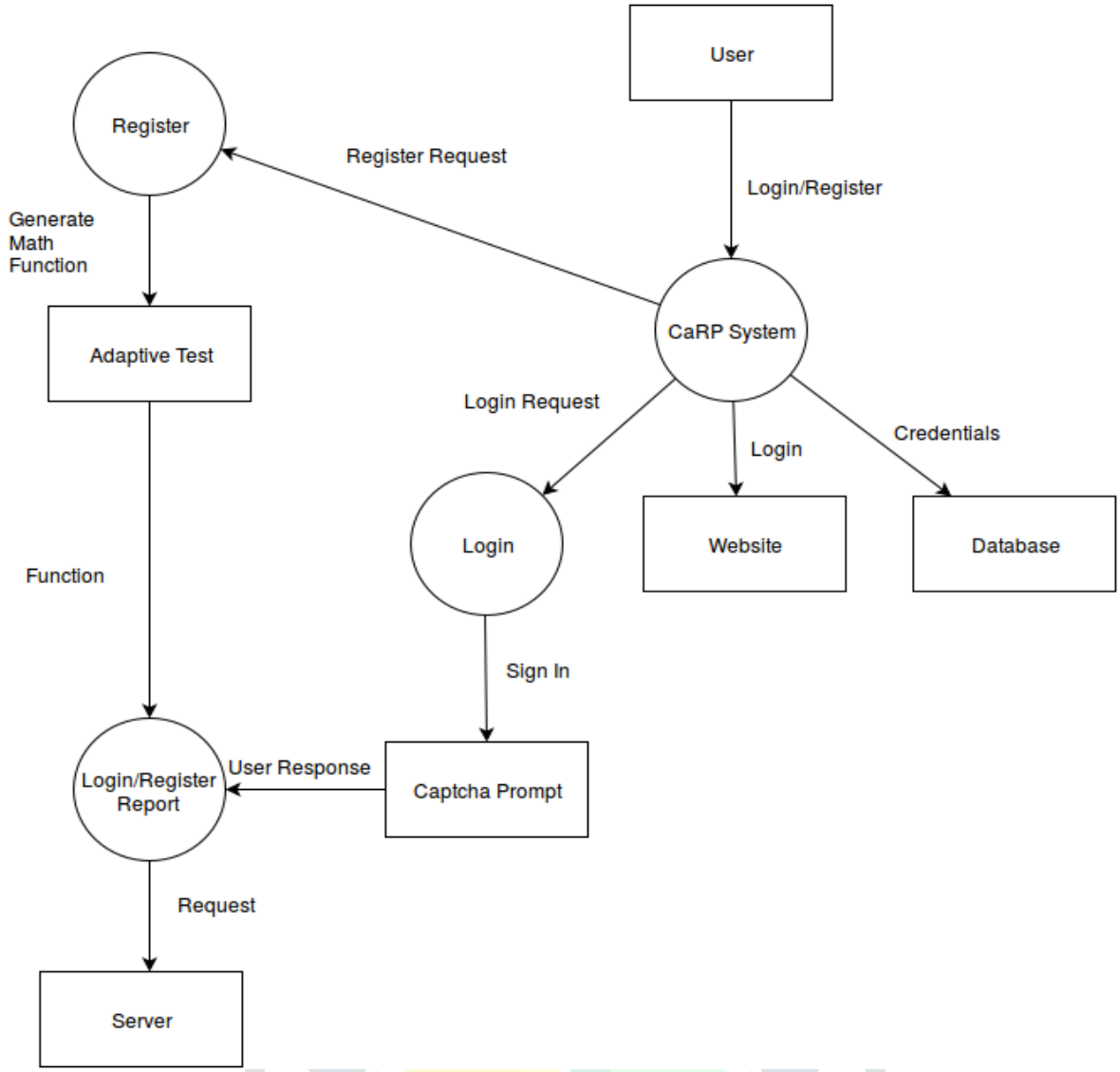

Fig 5: DFD Level 1

CONCLUSION

Thus we studied various paradigms for solving the critical issue relating to traditional password schemes. Though these techniques are making passwords more secure and dynamic, they also have their own drawbacks. We also over viewed an architecture of a proposed system which infuses machine learning with existing paradigm resulting in efficient password scheme.

REFERENCES

[1] Pooja Jaiprakash Kulkarni, Dr. G. M. Malwatkar, "The Graphical Security System by using CaRP", 2015 International Conference on Energy Systems and Applications (ICESA 2015), Nov 2015

[2] Anjitha K, Rijin I K, "Captcha As Graphical Passwords-Enhanced With Video-Based Captcha For Secure Services", Applied and Theoretical Computing and Communication Technology (iCATccT), 2015 International Conference, 29-31 Oct. 2015

[3] Vikas K. Kolekar, Milindkumar B. Vaidya, "Click and Session Based—Captcha as Graphical

[4] Password Authentication Schemes for Smart Phone and Web", 2015 International Conference on Information Processing (ICIP), Dec 2015