ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.7

A Survey on Secure Login Authentication System using Captcha Based Graphical Password Technique

Ganesh .D. Satkar[1], Vrushali Desale[2]
ME Student[1], Assistant Professor[2]
Department of Computer Engineering
Dr. D.Y. Patil Collage of Engineering, Ambi, Pune, India

Abstract:
Now a day, vulnerability is a major issue in infor- mation and computer security. The use of internet is increasing day by day. The user selects a password for security purpose, that password is text or graphical passwords. Mostly user uses text password because that are easy to remember, but the main drawback of using a text based password and graphical password is vulnerable to many attacks. So another technique is developed which is captcha. To overcome the limitations of the captcha new technique is developed which is CaRP (Captcha as Graphical Passwords).CaRP is a combination of captcha and graphical password. It is clicking an event which is performed at various points on image in the sequence to get a new password. In this system, Animal gird is used for user authentication, which is a type of CaRP techniques and Login history is used for transaction system for enhancing the more security level primitives.

Index Terms: password, password, CaRP, Captcha, security primitive, Animal grid, Login history.

I. INTRODUCTION

Security is the most important factor in an information security program for authentication. The text-based and Graphical passwords are used in the authentication process, but the best alternative for text-based password is a graphical password. The graphical password can reduce the burden of human memory as human mind to remember graphics and images better. Graphical passwords are vulnerable to shoulder surfing and spyware attacks, password, registration and log-in process needs more storage space. So the best alternative to graphical scheme is CAPTCHA (Completely Automated Public Turing-test to tell Computers and Humans Apart). Captcha is a type of challenge-response is generated by a human not by a computer. It is a program that generates and grade tests that are human solvable, but current computer programs do not have the ability to solve them. A new security primitive namely, a novel family of graphical password systems builds Captcha technology that is called a Captcha as graphical Passwords (CaRP). CaRP is click based graphical passwords, in which an order of clicks on an image is used to get a password. Contrasting other click-based graphical passwords, images used in CaRP are Captcha challenges and a new CaRP image is generated for every login attempt. The application where captcha as a graphical password is used is:

i) The captcha as graphical password is used in many internet applications specifically in the e-backing application, where users had to solve the different captcha at each login.

ii. By using the carp the entry of spam emails are reduced. Here the email service provider uses the captcha as a graphical password to log into the system so the spam bots cannot log into the system because they are not able to solve the captcha Authentication allows users to confirm their identity for any web application. The three major areas where human computer interaction is important that are Authentication, Security operations, and Developing secure systems. We focus on the authentication and transaction problem. A password is used for authentication, which are used to control access to a resource. The password is kept secret from unauthorized access, and those who want to gain access to the resource are tested on whether or not they know the password and they are granted or denied access accordingly. Traditional password is text based password. Many researchers have found an alternative approach that is graphical password. The password input is convenient as well as it is more user friendly in terms of memorability and recall ability. The main motivation of graphical passwords is the hypothesis that people are better at remembering images than artificial words. In addition, graphical password is an easier as well as more human friendly and memorization strategy recognition based memory used, instead of a recall based memory for textual password.

II. RELATED WORK

1. Graphical Password Techniques: Graphical password techniques are developed to overcome the limitations of text- based passwords. Graphical passwords consist of recognizing the images or sometimes to recognize the image and click the particular points or area on the image rather than typing the characters like text-based password. In this way, the problems that arise from the text-based passwords are reduced.

Graphical password techniques are categorized as follows: i) Recognition Based scheme ii) Recall Based scheme iii) Cued Recall Based scheme. A recognition based scheme has to select the certain number of images from a set of random images in an order as a password, and for authenticating the user has to identify (recognize) those images in a same order. There are three schemes under this system:

ii. Method 1: Dhamija and Perrig proposed a graphical authentication technique depends onto the hash visualization method. In their system, the user is asked to select a certain number of images from a set of random images generated by a program. The user will be required to identify the preselected images in order to be authenticated. ii Method 2: Sobrado and Birget developed a graphical password scheme work with the surfing shoulder problem. In the first technique, the system will show a number of passes-objects. A user needs to recognize pass-objects and click inside the outside hull formed by all the pass-objects for authentication.

iii. Method 3: Passface Real User Corporation developed these techniques. The idea is as follows: The user will be asked to choose four images of human facing as their future password security. In authentication stage, the user sees a grid of nine faces, consisting of one face previous chosen by the user eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. A recall-based scheme requires a user to reproduce something that he created or selected earlier during the registration stage.

Three techniques are: i) Method 1: Draw-A-Secret (DAS) Scheme Here the user will draw a simple picture on 2D grid. The coordinates of a grid are occupied by the picture are stored in the order of the drawing. During authentication, the user will be told to re-draw the picture. If the drawing touches the same sequence, then the user is authenticated.

ii. Method 2: Signature Scheme Here authentication is conducted by having the user drawing their signature using the mouse.

iii. Method 3: Pass-point Scheme Here the user will click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerances in the correct sequence [3].

Graphical password has some limitations: i) Password registration and log-in process take too long. ii) Require more storage space than text-based passwords.

2. *Captcha:* Completely Automated Public Turing Test to tell Computers and Human Apart [1] (Captcha) finds the difference in humans and bots in solving the hard AI problems. It is a test to check user is Human and not a computer device. Captcha has two types: Text Captcha which is recognition of non-character objects and Image Recognition Captcha relies on recognition of images.

i. Text Captcha: PayPal and Microsoft Captcha are both relied on background noise and random character strings to resist to automated attacks. The Captcha used by Google, Yahoo! All share similar properties, such as a lack of background noise of distortion for a character or word images and extreme crowding for an adjacent character. Random Captcha images are captured humanly reliably by site in the form of pixel, marginal probabilities and site by site covariance. EZ-Gimpy uses word images which employ character distortion and clutter.Personal print uses a low quality picture by degrading parameters to thicken, crowd, fragment and add noise to character images.

ii. Image Recognition Captcha: Captcha consist of a combination of images [6]. The user has to recognize the images given to him to solving the given puzzle problem. As shown in Figure.2 user has to select the cat images as the password characters.

3. *Captcha as Graphical Password (CaRP):* An Overview CaRP has a new image is generated for every login attempt even for the same user. Alphabet which is used in CaRP of visual objects (E.g. Alphanumerical characters, similar animals, etc.) to generate a CaRP image, which is also a Captcha challenge. A Recognition-based CaRP technique used password is in a series of visual objects alphabet. Per view for the traditional recognition based on graphical password security, recognition based CaRP seems to have access to an infinite number of different visual objects.

We present two recognitions based CaRP techniques and a variation next. A recognition-recall CaRP, Password is a sequence of some invariant points of objects. An invariant point of an object is the point that has a fixed relative position in different incarnations of the object and it can be uniquely identified by users or humans no matter how the object appears in CaRP images.

A Recognition-based CaRP technique used password is in a series of visual objects alphabet. Per view for the traditional recognition based on graphical password security, recognition based CaRP seems to have access to an infinite number of different visual objects. We present two recognitions-based CaRP techniques and a variation next.

i. ClickText: ClickText having a recognition-based CaRP scheme. CaRP techniques use CAPTCHA as its underlying the principle. Alphabet set of ClickText comprises alphanumeric characters. A ClickText password is a series of characters in the alphabet.e.g. =DEF@2SK78, which is a similar to the text password. A ClickText image is totally different from usual CAPTCHA as all the characters of alphabet set are to be included in the CaRP image. The underlying CAPTCHA engine generates such CaRP image. When image is generated, then each characters location in the image is recorded which would be used in the authentication. Characters can be put randomly in 2D space in these images which changes from text CAPTCHA where characters are typically ordered from left to right in order for users type them sequentially Fig. 3 shows a ClickText image with an alphabet of 33 characters [1].

ii. ClickAnimal: ClickAnimal is a recognition-based CaRP technique. It has an alphabet of similar animals such as dog, pig, like that. The password in this technique is a sequence of animal names like = Cat, Dog, Turkey,.. Most of the models are created or built for each and every animal. The CAPTCHA generation activity where in 3D models are used to get 2D models by applying different types of views, colors, and optionally distortions are used for generating the Click Animal image. The final resulting 2D animals are then arranged on cluttered backgrounds like grassland. The number of similar animals is less than the number of available characters. Some time some animals may be overlapped by some other animals in the image, but their core parts are not overlapped in order for

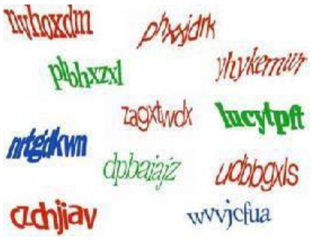


Figure.1. Captcha Images

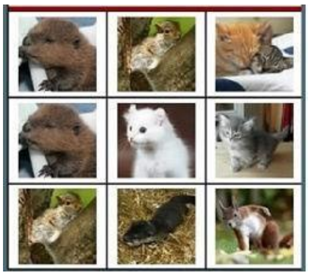


Figure.2. Image based captchas

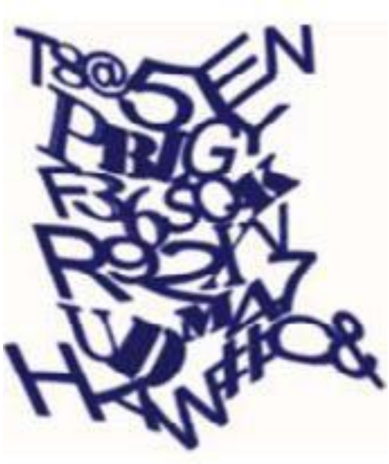


Figure.3. ClickText CaRP Scheme

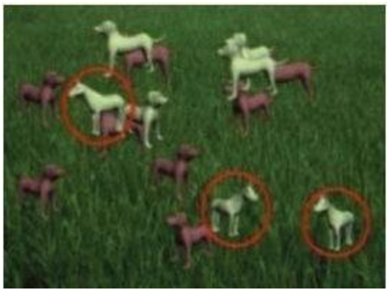
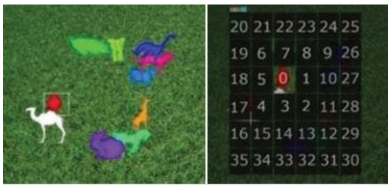


Figure.4. Click Animal CaRP Scheme



Figur.5. A Click Animal Image(Left) and 6*6 Grid (Right)Determine by Red Turkey's Bounding Rectangle

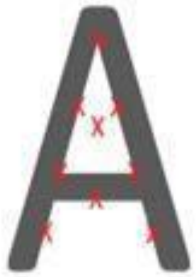


Figure.6. Some invariant points (red crosses) of "A"

iii. TextPoints4CR: CaRP scheme presented up to now, the coordinates of user-clicked some points are sent directly to the authentication server during its authentication. For more complex rules, say a challenges and response authentication protocol, the response is sent to the authentication server Instead. Text Points sometime its can be modified to fit challenge response authentication. This variation is called as Text Points for Challenge Response or also TextPoints4CR. CarRP have some benefits given below: i) CaRP to offer protection against Automatic Online Guessing Attacks on passwords. ii) It offers security against Human Guessing Attacks. iii) It offers protection against Shoulder Surfing Attack. iv) It offers security against spam emails sent from a Web email service. v) It offers security against spam emails sent from a Web email service. CaRP has some limitation: i) CaRP scheme is vulnerable to phishing attack because user-clicked points are sent to the a authentication server. ii) CaRP is vulnerable if both the image and user-clicked points can be captured.(if client is compromised)

III. PROPOSED SYSTEM OVERVIEW

A. Problem Statement

: To improve the CaRP System with valid authentication and enhance the Security by using images of different level of difficulty based on CaRP Technique with an animal grid as graphical password and generate the Login History image for the transaction.

B. System Architecture

As shown in the above fig.7 the system will work as follows:

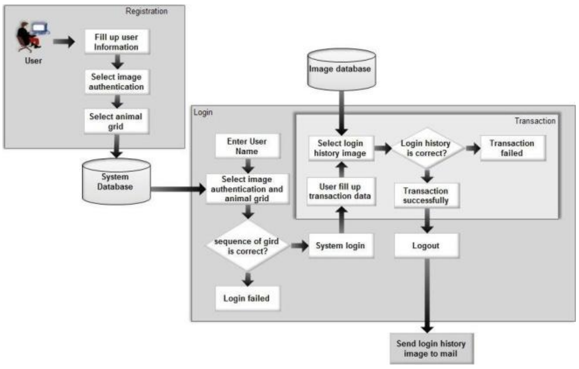

Registration
User
Fill up user Information
Select image authentication
Select animal grid
System Database
Image database
Login
Transaction
Enter User Name
Select image authentication and animal grid
sequence of gird is correct?
Login failed
System login
User fill up transaction data
Select login history image
Login history is correct?
Transaction failed
Transaction successfully
Logout
Send login history image to mail

Figure.7. System Architecture

- **Registration Process**

First user starts the registration process, where the user fills up the information and selects at least 6 images from animal grid. The animal grid image is generated by the system from the system's database. Then the selected graphical password by the user is saved in database.

- **Login Process**

During the login process the first step is user entered the username and selects the image which he has selected during the registration process. Then the user selects

- **Transaction Process**

After the successful login user will actually enter into the system where users can perform the transaction. For that transaction user will enter details when he submits his transaction at that time 6 login history will be displayed. When the user selects the correct imagethenonly transac- tion is successful otherwise not. The login history image will be sent to users mail after logout.

IV. EXPERIMENTAL RESULTS

We have tested our results in a suitable testing environment, where we have tested the performance of the system during the following three scenarios:.

- Graphical passwords
- Animal grid
- Login history

The figure 8. show the performance of the system during the time. The Figure shows the total time taken by the system, how enhanced the authentication of users. Figure shows that as early when only use the password for security purpose, then very less authentication is done. After that when system enhancing then security or an authentication is very high for the system. Our system uses the animal grid as well as the login history image of last login time and logout time, which is more secure from other system which have already used like pass-point, click-text, password. The figure 9. shows the performance of the system as well as how much people say that system is more secure than previous systems in the form of a percentage. Animal grid to login history image provides high security, 50 percent confirm that system enhancing the security as compared to the other

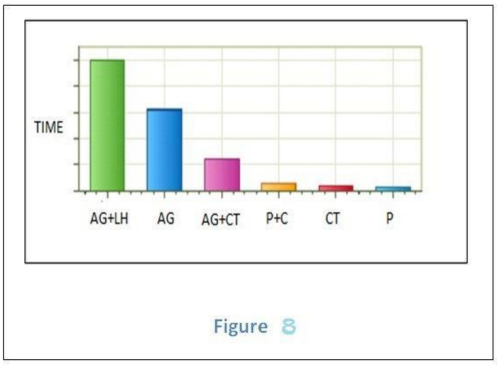


Figure. 8. Performance of the system during time

System. When use the only animal grid as graphical password security authentication 30 pecent people says that system is secure. And the little bit response for password and click text techniques. Enhancing the system with time and adding technology with respect to their hardness.

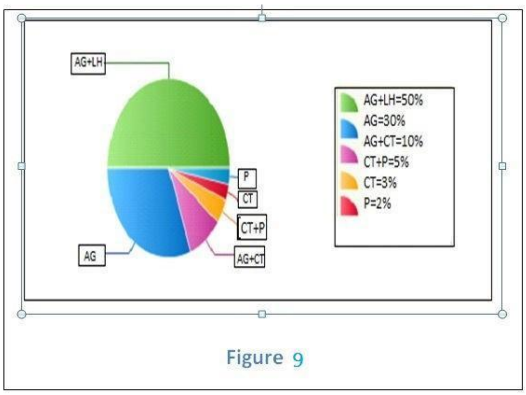


Figure.9. Performance of the system

V. CONCLUSION

In this paper, we have surveyed various security techniques such as textual password, graphical password, Captcha password and CaRP technique. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP schemes are classified as Recognition-Based CaRP and Recognition-Recall CaRP. We have discussed Recognition- Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques in this paper. Current graphical password techniques are an alternative to text password, but are still not fully secure. As a framework, CaRP does not rely on any specific CAPTCHA scheme, but CAPTCHA scheme is broken, then a new and more secure scheme appears is a CaRP scheme. Due to reasonable security and practical applications, CaRP has best potential for refinements. The usability of CaRP can be further improved by using images of different layers of difficulty based on the login history of machining.

ACKNOWLEDGMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. I also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

VI. REFERENCES

[1]. Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, Captcha as Graphical PasswordsA New SecurityPrimitive Based on Hard AI Problems , IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2015.

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

[3]S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, PassPoints: Design and longitudinal evaluation of a graphical password system, Int. J. HCI, vol. 63, pp. 102127, Jul. 2005.

[4]L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, CAPTCHA: Using hard AI problems for security, in Proc. Eurocrypt, 2013,

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

[6]P. C. van Oorschot and J. Thorpe, On predictive models and userdrawn graphical passwords, ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 133, 2008.

[7]H. Gao, X. Liu, S.Wang, and R. Dai, A new graphical password scheme against spyware by using CAPTCHA, in Proc. Symp. Usable Privacy Security, 2009, pp. 760767.

[8]. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, Against spyware using CAPTCHA in graphical password scheme, in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 19.