CAPTCHA: Novel Approach to Secure User

Ms. Mrunali S.Sonwalkar
Dept.of Computer science and engg.
M.B.E.S.College of engineering, Ambajogai. India
mrunali.sonwalkar@gmail.com

Abstract

Now a day's internet security is a major issue to tackle. Authentication is the heart of the secure system. Most common method used for authentication is username and password. Due to vulnerabilities of this traditional authentication method, some improved secured approach is required. This paper focuses on use of CAPTCHA as an authentication. The method proposed in this paper is CaRP i.e. CAPTCHA as a graphical password. CaRP can be used as a CAPTCHA and a graphical password. CaRP is click-based graphical passwords. The idea of CaRP is simple but generic. In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects to generate a CaRP image. The algorithm is used to verify user's identity with the help of image selected by user and thus provides security to individual user's account as well as protect user's data. Finally graph is used to illustrate how difficult it is to guess the password while login. Another graph is used to illustrate how user friendly our system is by comparing it with other existing methods while remembering the password.

1. Introduction

The internet is playing extremely important role in our daily life. As the usage of internet is growing rapidly, the security constraints used over internet need to be updated frequently. One of the major issues over internet security is the authentication of user. Before being part of any transaction system, user has to authenticate himself. If sensitive information is given to wrong identity, the entire security of the system will collapse. Authentication is the process of confirming user's identity over internet. Authentication is one of the five pillars of information assurance (IA). Authentication is used to determine whether the user should be given access to the system/resource. The common factors associated with authenticating user over internet fall into three categories: something the user knows, something the user has, and something the user is. Each authentication factor covers a range of elements used to authenticate or verify a person's identity.

Generally, the most common authentication method is the conventional username and alphanumeric password. A password is a form of secret authentication that is used to control access to data, which is usually kept secret from any other user [1]. It is kept secret from unauthorized users, and these wishing to gain access are tested and are granted or denied the access based on the password according to that. Passwords are used from ancient times itself as unique code to detect the malicious users. In modern times, passwords are used to limit access to protect computer operating systems, mobile phones, others etc.

Another method used for authentication, which is becoming more popular now a days is use of CAPCHA.CAPCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans apart. CAPTCHA systems are used as a security mechanism in web applications. CAPTCHAs are a standard security mechanism used on many websites to protect online services against misuse by automated programs. CAPTCHAs are designed to be simple problems that can be quickly solved by humans, but are difficult for computers to solve. The concept of CAPTCHA is based on the ability of humans to do certain tasks which computer programs cannot do. These common tasks are, asking users to type a distorted text image or choose a particular picture from many displayed pictures. The user is required to provide a correct response to the test and then the user is allowed to access the work. When a correct response is received, it is believed to be an authenticated user's responses.

1.1 Types of CAPTCHA:

There are many types of CAPTCHA systems have been explored which are categorized into four types:

1.1.1 Text based
1.1.2 Image based
1.1.3 Audio based
1.1.4 Video based

1.1.1 Text-based CAPTCHA:

Text based CAPTCHAs is a very simple to implement. It is very effective and requires a large question bank. The text based CAPTCHA is possible to identify the character and digit through Optical Character Recognition (OCR) technique. Text-based CAPTCHA is deployed in famous websites, examples Yahoo, Hotmail, Gmail, YouTube, PayPal etc. Gimpy, Ez-Gimpy, Baffle-Text and MSN-CAPTCHA are the types of Text-based CAPTCHA.

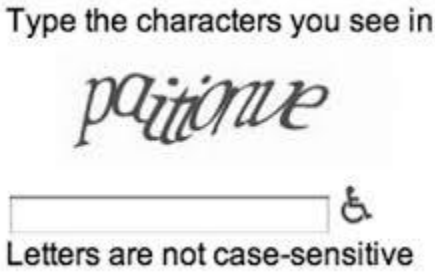

Figure.1.1.1 Text –based CAPTCHA

1.1.2 Image-based CAPTCHA:-

Graphics-based CAPTCHAs are challenge-tests in which the users have to guess those images that have some similarity. The advantage of image based CAPTCHA is that pattern recognition is hard AI problem and therefore it is difficult to break this test using pattern recognition technique. In the graphics based CAPTCHA, the CAPTCHA tests in which the users need to figure those pictures that have some similarity. ESP Pix is a first image based CAPTCHA and it is accessible just in English language. It utilized a bigger database of images and animated pictures of regular items. In general, image based CAPTCHAs present a visual pattern or idea that the user needs to distinguish and act appropriately.

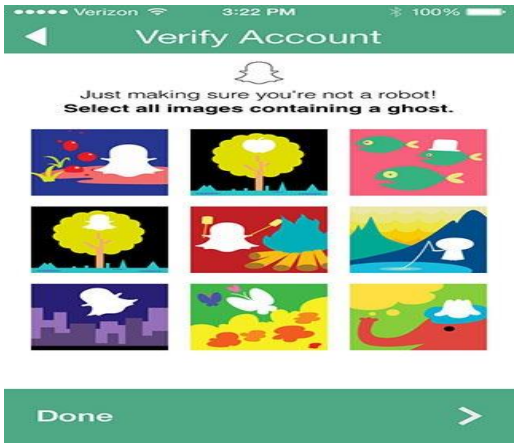

Figure 1.1.2 Image –based CAPTCHA

Some types of image-based CAPTCHA are Pix and Bongo :-

Pix CAPTCHA use a large database of photographic and animated images of daily objects. Set of images are shown to user, all related with the same concept or object .The user must then enter the concept or object to which all the images belong. For example – what is the similar feature among the pictures that is shown in Figure 1.1.2.

Bongo CAPTCHAs is developed by Mikhail M. Bongard. In this type user has given a visual pattern recognition problem for solving. Bongo contains two series of blocks, the left block series and the right block series. The blocks in the right series differ from those in the left, and the user should identify the correct blocks and group them together.

1.1.3Audio-based CAPTCHA:-

Audio-based CAPTCHAs are based on the sound-based systems. These CAPTCHAs are developed for visually disabled users. It contains downloadable audio-clips. In this type of CAPTCHA, first the user listens and after that submits the spoken word. This is a sound based CAPTCHA. They takes an arbitrary grouping drawn from recordings of words or numbers, consolidate them and include some disturbance/noise to it and given to the user. The user listen the sound clips and after that sort the talked word in the answer box and afterward submits it. Eco is the first audio based CAPTCHA was actualized by the Nancy Chan from the City University.

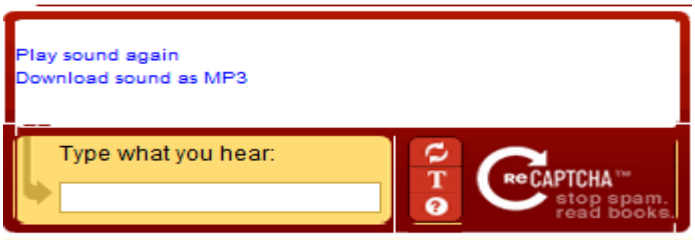

Figure 1.1.3 Audio –based CAPTCHA

1.1.4 Video-based CAPTCHA:-

In video-based CAPTCHAs, three words (tags) are provided to the user which describes a video. The user's tag must match to a set of automatically generated ground truth tags then only the test is said to be passed. A video can be taken from any public database that has three words used to describe the video. As the video plays words may submit, i.e. the user does not have to

wait for the video to finish before submitting their three words. The user's tag has to match to automatically produce ground truth tags then only the test is passed. Although video CAPTCHA is limited, both commercial and academic application does exist.

Figure 1.1.4 Video–based CAPTCHA

1.2 CAPTCHA in Authentication

CAPTCHA and password is used as a general method for authentication. A protocol is designed based upon use of CAPTCHA as a password, which is called as CAPTCHA based authentication protocol (CbPA). The CbPA-protocol in requires solving a CAPTCHA challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. An improved version of CbPA-protocol is proposed in by storing cookies only on user-trusted machines and applying a CAPTCHA challenge only when the number of failed login attempts for the account has exceeded a threshold [2]. The same protocol is further improved by making changes in the range of threshold values, as a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time slot. With the help of this method user has to prove its own authentication within a specific time limit.

2. Related Work

In Bin Zhuet.al [3] presented a new security primitive based on hard AI namely, of graphical password system built on top of CAPTCHA technology, which called a CAPTCHA as a graphical password schema. A Number of security problems address using CaRP , such as online guessing attacks as well as relay attacks and if combined with duel-view technologies , shoulder surfing attacks. It also implements CaRP, a new security primitive relying on unsolved hard AI problems. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints that often leads to weak password choices. CaRP offers reasonable security and usability and appears to fit well with some practical applications for improving online security**.**

Rohini A. Dodamani and Prof. Vivekanand Reddy[4] proposed CaRP scheme. In CaRP i.e. CAPTCHA as graphical Passwords, CAPTCHA and graphical password is combined and used as a single entity for authentication. The CaRP schemes are actually click-based graphical passwords with the CAPTCHA technique used in a way that a new image is generated for every login attempt even for the existing user just as CAPTCHAs change everytime. CaRP uses an alphabet set. They have used visual objects instead of actual characters, i.e. a visual depiction of alphanumeric characters or might be some objects is used for the CaRP image generation which

actually turns out to be a CAPTCHA challenge. One of the noticeable difference between normal CAPTCHA and CaRP images is that all objects of an alphabet set for a CaRP scheme are included in every image challenge unlike normal CAPTCHAs where only a part of alphabet set is used.

A Recognition-based technique is proposed by Dhamija and Perrig as a graphical authentication method which uses Hash Visualization technique [5]. 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. The user will be required to identify those selected images in order to be authenticated. The time taken for this process 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 images database can be time consuming for the user.

P.Dunphy and J.Yan proposed a technique, called "Draw- a - secret (DAS)" [6], which allows the user to draw their unique password. A user is asked to draw a simple picture or 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 the password on 2D grid. During login process, the user is asked to re-draw 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, it fails. They also suggested that given reasonable-length passwords is in a 2D grid, the password space of DAS is larger than that of the text based password space. They introduced the concept of graphical passwords and also observed the possibility of a brute-force attack using such passwords.

Another novel approach is suggested by, Jayshree Ghorpade et. al [7].They presented first catalogues of existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. They also introduce the concept of graphical password which can be classified into three categories that are recognition based graphical password cued based graphical password and recall based graphical password. In recall based graphical password, user are required to recall a password without any cue, a graphical password is formed using group of pictures which need to be combined together to authenticate a user. In recognition based graphical password the user required to recognize and then select a set of preselected images from large set. In cued recall based graphical password an external cue is provided to help memorize and enter a password.

Bin B. Zhu et. al [8] studied the design of image recognition CAPTCHAs (IRCs).They have examined all IRCs schemes known to us and evaluate each scheme against the practical requirements in CAPTCHA applications, particularly in large-scale real-life applications such as Gmail and Hotmail. Then they presented a security analysis of the representative schemes which are identified. They have also provided a simple but novel framework for guiding the design of robust IRCs. The images which are used for CAPTCHA as well as CAPTCHA generation can be done automatically.

3. Proposed System

There are numerous ways available to make system secure using CAPTCHA. All the method presented before uses different approaches to form a CAPTCHA as a password. Instead of using text based CAPTCHA, the technique focused in this paper uses graphical password authentication, making a graphical CAPTCHA[9]. A graphical password authentication system works by allowing the user to select images, in a specific order, presented in graphical user interface (GUI).One of the benefit behind this approach is). A graphical password is easier than

text based password for most people to remember. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words rather than the recommended combinations of characters or alphanumeric characters.

The basic concept used in this paper is CaRP (Captcha as a Graphical Password). CaRP is click-based graphical passwords, where a sequence of clicks on an image is used 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. The idea of CaRP is simple but generic. CaRP can have multiple instantiations. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in.

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects to generate a CaRP image, which is also a Captcha challenge[10]. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes.

CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space.

The algorithm used to generate new image for every new login attempt is as follows:

3.1 Algorithm:-

Step 1 Start

Step 2 User can register by username, password, Email-id, Contact no.

Step 3 Computer generate graphical Captcha for registered user.

Step 4 User will select Captcha.

Step 5 Authentication of User:

User will enter his details which he entered at the time of registration.

Step 6 Computer program ask the user to choose the correct graphical Captcha.

Step 7 User selects the graphical Captcha.

Step 8 Is selected image Captcha is correct?

1. If Yes

Step 9 User can access his account.

Step I: User can Upload & Download file From File Storage.

Step II: If User Want Security for Individual File.

Login step -User click on point of image & Set the security for individual file.

2. If NO

Step 10 User can login again.

Step 11 Stop.

4. Performance Evaluation

The performance of the CaRP is compared with other three user authentication methods. It shows how user-friendly the proposed system is and whether it matches the security of the system and how difficult it is to guess the password while login. The analysis of the system's behavior is represented with following charts.

Figure 4.1 shows the login time required over the 40 participants successful login attempts. It also shows the maximum and minimum login times for each scheme. Animal Grid has maximum login time; whereas CaRP and Pass Points had similar average login time. Text had a much shorter average login time than the other schemes. A participant's login time in each trial was recorded by the server. The login time is defined as the duration from the time when the server received a login request to the time when the server gave its response to the login request, which includes the time to enter user ID and password, to generate a CaRP image, and to communicate between the server and a participant's browser.

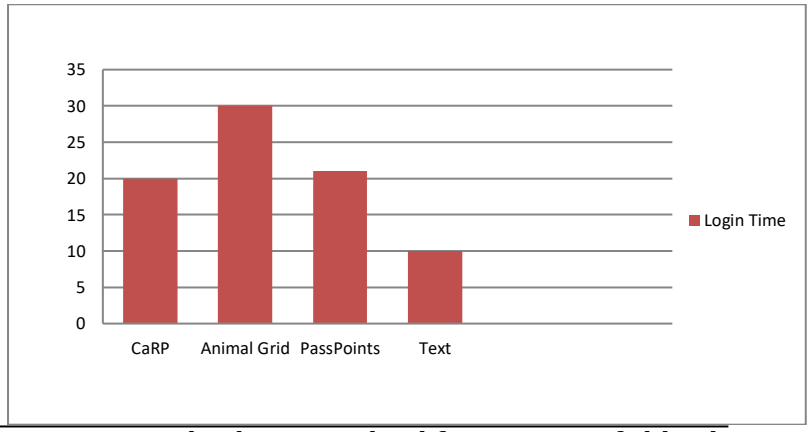

Figure 4.1. Login time required for successful login

CaRP is also compared with other authentication methods to test the password memorability for each scheme. The time required for recalling passwords using various method is shown in Figure 4.2. The scale used for comparison is from 1 to 5 indicating easy to difficult. The chart shows that Animal grid has highest difficulty in remembering the password, where as PassPoint and Text has moderate one. CaRP less difficulties in remembering the password as compared to other three.

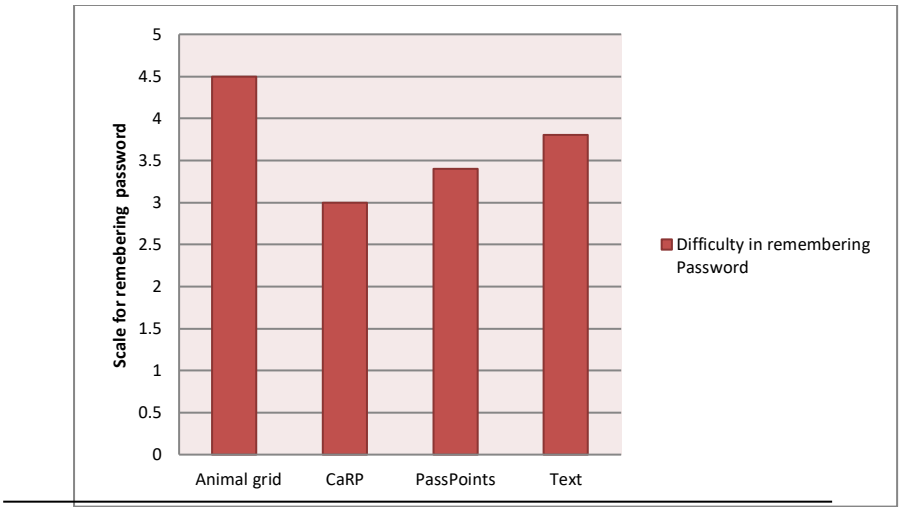

Figure 4.2 Time required for recalling passwords of various methods

5. Conclusion

CaRP is both a Captcha and a graphical password scheme. The idea of CaRP introduces a new family of graphical passwords which adopts new the techniques to overcome password guessing attacks. The experimental results proved that, the login time for CaRP is average; also the difficulties for recalling the password using CaRP are also less as compared to other approaches. CaRP provides strong security and usability policies. CaRP has good potential for refinements, which call for useful future work.

References

[1] V. Bhusari, "Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153

[2] A. Jenifer Jothi Mary , L. Arockiam, "A Framework for Aspect level Sentiment Analysis of Academic Results Data ", International Journal of Recent Trends in Engineering & Research (IJRTER)

Volume 02, Issue 07; July - 2016 [ISSN: 2455-1457]

[3] Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014

[4] Rohini A. Dodamani and Prof. Vivekanand Reddy, "Authentication Security Scheme Using Hard Ai Based Graphical Password on Captcha Technology", International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 02, Issue 07; July - 2016 [ISSN: 2455-1457]

[5] M. Dailey , "A text graphics character CAPTCHA for password authentication", 2004 IEEE Region 10 Conference TENCON 2004, 24-24 Nov. 2004.

[6] Zarina Mohamad, Lim Yan Thong, Aznida Hayati Zakaria, Wan Suryani Wan Awang, "Image Based Authentication using Zero-knowledge Protocol".

[7] Jayshree Ghorpade, Shamika Mukane, Devika Patil, Dhanashree Poal, Ritesh Prasad, "Novel Method for Graphical Passwords using CAPTCHA International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-5, November 2014

[8] Bin B. Zhu , Jeff Yan , Qiujie Li , Chao Yang , Jia Liu , Ning Xu , Meng Yi , Kaiwei Cai, "Attacks and design of image recognition CAPTCHAs," inProc. ACM CCS, 2016, pp. 187–200.
[9] Rosa Lin Shih-Yu Huang, Graeme B Bell, Yeuan-Kuen Lee, "A New CAPTCHA Interface Design for Mobile Devices", 12th Australasian User Interface Conference, AUIC 2011.
[10] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2017.
[11] Susan Wiedenbeck,, Jim Waters, Jean-Camille Birget, Alex Brodskiy , Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", Int. J. Human-Computer Studies 63 (2015) 102–127.
[12] M. Szydlowski, C. Kruegel, and E. Kirda, "Secure input for web applications," in Proc. ACSAC, 2012, pp. 375–384.