An Efficient User Authentication using Captcha and Graphical Passwords-A Survey

S. Karthika, Dr. P. Devaki

[1]PG Student, Kumaraguru College of Technology, Coimbatore-Tamilnadu, India

[2]Associate Professor, Kumaraguru College of Technology, Coimbatore-Tamilnadu, India

Abstract: ***CAPTCHA is an acronym for Completely Automated Public Turning Test to tell Computers and Humans Apart. Captcha is one of the widely used techniques for preventing malicious program from accessing the web resource automatically. Now a day's for web security there exists different type of Captcha such as text Captcha, image Captcha, audio Captcha and video captcha . In this paper online security scheme is constructed with text and graphical passwords. Captcha and Graphical passwords are integrated and a novel family of graphical password systems built on top of Captcha technology is called as Captcha as graphical passwords (CaRP). The CaRP scheme is enhanced with more attack handling mechanisms that improves the level of security in online application system and also provides better authentication.***

Keywords: Captcha, Graphical password, Authentication

1. Introduction

Internet has become an indispensable part of daily transactions including shopping, education, Commerce and industrial sector. All these transactions mainly needs to enter individual information in certain registration forms and then only the user is allowed to access that website. But some individuals" fills wrong information and access the website by developing programs which make the false registration. It results in the wastage of web resources. So in this way the malicious programmers or robots try to deny the services used by the regular users. These attacks are called "Denial of services"[14].

There are various methods introduced to prevent these attacks. It is difficult for humans to examine the huge and bulky data of registration. Some methods are implemented with the help of computer in order to distinguish human users from computers. To distinguish between human and machine a test known as Turing test is used in which the right judgment is made by providing intelligence to computer. In turing test human and machine are in different rooms and a human judge has to decide who is responding a machine or human by asking number of questions. CAPTCHA is turing test with a difference that computer guesses whether it is a human or bots.

The CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) [2] is a system, CAPTCHA is a distorted image containing short text. It is displayed in such a format so that only human eyes can recognize the alphabets clearly. At the time of registration, such image is displayed on the form and the user is asked to write the same text in given text field. The robots fail to recognize the short text. Thus, website owners can prevent robots from registration and can ensure that all the members using free services are humans. Thus CAPTCHAs prevent automated posting to blogs and forums. CAPTCHAs can be used further in avoiding spam emails.

It is widely accepted that a good CAPTCHA must be both robust and usable. The robustness of a CAPTCHA is its strength in resisting adversarial attacks, and this has attracted considerable attention in the research community [18,19]

There are some properties defined for the development of CAPTCHA

- **Automated:** Computer program should be able to generate and grate the tests.
- **Open:** The database and algorithm used to generate and grade the tests should be made public.
- **Usable:** Humans must able to solve the test in reasonable amount of time. The effect of users language, physical location, education and perceptual abilities should be minimal.
- **Secure:** The program generates the test should be difficult for machines to solve by using any algorithm.

A CAPTCHA[14] system must satisfy the following three characters:

1) Human can recognize the contents and pass it easily.
2) It is invoked to prevent robots to pass the system or to increase the processing cost through continuous attack.
3) It should be generated easily and quickly.

CAPTCHAs have several applications for practical security, Preventing Comment Spam in Blogs, Preventing Dictionary Attacks, Search Engine Bots, Worms and Spam, Protecting Website Registration, Protecting Email Addresses from Scrapers, Online Polls.

CAPTCHA is an authentication process based on challenge-response authentication. CAPTCHA provides a mechanism with the help of which a user's can protect themselves for spam and password decryption by taking a simple test. In this test a user will see either an image or a text which are normally distorted. The user is supposed to enter the pattern exactly as shown to him if the CAPTCH is based on text. If the CAPTCHA is based on image the user is supposed to enter the correct name of the image which correctly

symbolizes the image. CAPTCHA is used where authenticated access is the primary concern. Various web services like Yahoo, Google, and Bing etc. use CAPTCHA to differentiate between an authenticated user and a malicious program. CAPTCHAs are also used in the sites which provide access to sensitive data, such credit card accounts and banks.
There are three basic properties that CAPTCHAs must satisfy. They are

1. CAPTCHAs should be easy for human user pass.
2. It should be flexible enough so that a tester machine easily generate and grade it.
3. Must be hard enough for a bot to pass.

There are many types of CAPTCHA[13] systems have been explored. Which are categorized into four types:
(1) Text based Captcha
(2) Image based Captcha
(3) Audio based Captcha
(4) Video based Captcha

Text based Captcha:
Text based CAPTCHAs is a very simple to implement. It is very effective and requires a large question bank. In Text based captcha the Number of classes of characters and digits are very small so the problem occur for user to identify the correct characters and digits. The text based captcha is possible to identify the character and digit through Optical character recognition (OCR) technique [16,20]. In Text based CAPTCHAs simple asked questions like as based on arithmetic equation.

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.

Audio 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**.**

Video based Captcha:
Video CAPTCHA is a newer and less commonly seen CAPTCHA system. 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.

Application Of All Types Of Captcha
There are number of applications of CAPTCHA[13] on the web which are defined as follows.
(1) **Registering the web form:** There are many sites on the internet which provides free registration to avail their services. But they are susceptible to web bots. It may come into the form of scripts which can register thousands of email accounts on the internet, thus wasting the precious space of web.
(2) **Online polling sites:** These sites takes user's response or feedback in the form of questionnaires. To ensure that only human makes the response they make use of CAPTCHA.
(3) **To avoid web crawling:** If a site doesn't want to get indexed by a search engine then they can make use of CAPTCHA.
(4) E-Ticketing.
(5) Preventing Dictionary Attacks and E-mail spam.

2. Related Work

There are many Captcha techniques are design to provide better authentication for online application. CAPTCHA can provide the ease of access to the user and highest level of security by preventing the BOT attacks. But there are drawback existing in each Captcha technique such as text captcha, audio captcha and so on. And several kinds of attacks are also possible on the captcha .To overcome these drawback there is need to create a efficient Captcha technique to provide better authentication and protects the Captcha from different kinds of attacks using graphical password for Catcha. Thus this help us to protect Captcha from attacks and also reduces the risk of providing low level authentication.

3. Literature Review

Authentication is an important thing in online applications. The attacker may try to capture the user authentication information through keyboard hooking. To overcome this problem a password input method is based on entering the password using mouse click or touch pad on the Captcha images[15].The mapping is random. The pixels are consisting of CAPTCHA. The users password during transmission are exploited to get the discrete logarithmic problem such that the password can be transmitted securely.

For phising detection and prevention a scheme called Anti-Phishing Image Captcha validation scheme using visual cryptography is used which prevents password and other confidential information from the phishing websites[12] .To increase more security "Blowfish Algorithm" can be used to divide the original image captcha into many blocks and rearrangement can be done. Then "Splitting and Rotating Algorithm"[21] can be used to rotate the rearranged blocks. The original image captcha id divided into two different image shares by manipulating the black and white pixel value of the image captcha. Part of the image share will be stored in the servers such that the original image captcha can be revealed only when both (client,server) of the shares are simultaneously available. The individual share images do not reveal the identity of the original image captcha. Once the original image captcha is revealed after merging different shares, which can be used as the password.

Password guessing resistance protocol (PGRP)[1] is used which is used to protect to the text password from brute force and dictionary attack. It is also used to control user verification attack. The PGRP first checks the checks the IP address and username with whitelist if it is not in the white list it enforces ATTs (Automatic Turing Test) after few login attempts if the login is from unknown machine and stores the IP address in the blacklist. It allows a high number of failed attempts from known machines without answering any ATTs.

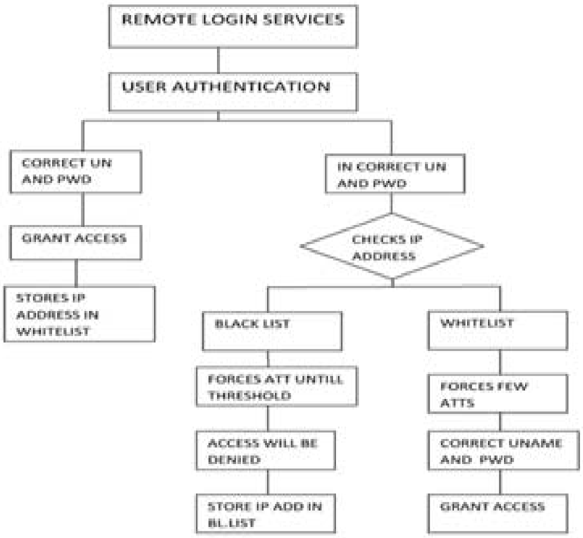

Image Recognition CAPTCHA (IRC) scheme is designed with object recognition with surrounding context information and Context-based Object Recognition to Tell Computers and Humans Apart (Cortcha) scheme is used[2]. In CORTCHA an image database is created. On the selected image segmentation and object selection is performed and finally image inpainting is done for the purpose of making the user to identify correct object challenging. CORTCHA is scalable and it is integrated with the text password. Any number of images can be added to the database. It nearly takes 122 seconds to create a challenge.

In [3] CAPTCHA Zoo interface scheme is tuned for the mobile devices. It designed to verify users in mobile services with CAPTCHA. Image is created by first generating a background image textured. Two visually similar kinds of animals are then randomly drawn over the background. The images are of 3-dimensional form which difficult for the adversary to find out the correct image when viewed from different angles. The user wants to select the correct targeted image . Improves the security of online systems that are accessed by mobile devices.The system supports mobile user verification only.

Persuasive Cued Click-Points (PCCP) scheme is used to construct graphical passwords where a Graphical password scheme is designed with viewpoint based mechanism. The user should select the less predictable password so when the user creates a password the images are slightly shaded except for a viewport. Users must select a click-point within this highlighted viewport . Viewport is positioned randomly. Better user interface design can influence users to select stronger passwords[4].

Quantitative analysis based PIN entry[5], mechanism is used to verify the users in which the system secures the personal identification number (PIN) entry against shoulder surfing attacks. Two methods LIN4 and LIN5 are used were LIN4 includes 4 rounds and LIN5 includes 5 rounds were first round is session key round and others are Pin entry round .Horizontal array of digits from 0 to 9 and another array of ten familiar objects. The user recognizes the symbol below the first digit of the PIN and followed by remaining digits of the PIN. The system supports textual characters only.

Window Clustering Algorithm and Dictionary Generation Algorithm are used in the attack analysis process which verifies the passpoint based graphical passwords with spatial pattern based attacks[6].These system indicates the chance of location pattern attacks. In window clustering algorithm the window size is fixed. In Dictionary generation the attacker plans to generate a dictionary consisting of subset of r-permutations.

In [7], Opportunistic Solving and Paid Solving methods are used which makes the system analyzes the schemes supported by the CAPTCHA-solving service providers. It is based on human assisted Captcha solving methods. Here the peoples are paid for solving CAPTCHA.

Hidden safety loophole mechanism is used in which the system uses the CAPTCHA in graphical passwords scheme. Spyware attacks are controlled by the system. Users are required to select and remember letter positions within the string of letters .These letter positions are the called pass-positions for each image. During authentication Users should enter the characters shown in the pass-positions.This system is resistant to the attack launched by the humans with spyware which also simultaneously preserves the graphical password scheme[8].

In [9], Covert attentional scheme on shoulder surfing attacks has the major role which is designed to control the shoulder surfing attacks in PIN entry. Let P denotes the set of four colors such that P = {black, blue, white, yellow}.The system also displays a set of ten digits, on the keypad with two split colors chosen from *P*. The user attends to the PIN digit and enters the either of its color through the color key. The user and the system repeat this procedure for *m* rounds that the PIN digit is identified by intersection and until all the PIN digits are identified. The required number of rounds is $m \times n$.

Multitouch gesture matching algorithm[10] is use to analyze the finger hand movements and it is to authenticate users in touch sensitive devices. This algorithm preprocess Multitouch gesture data by reabelling each and every touch point according to the corresponding fingertip in order to make the input comparable. It derives rotation and translation invariant features to represent the gesture. Dissimilarity score is calculated from the pairwise distance. The multitouch gesture is accepted if and only if the dissimilarity score is less than the predefined threshold.

Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. It combines both captcha and graphical password scheme for improving online security[11].It uses the technique called Text4CR(Text for Challenge Response). To enter a password a user must identify the objects in a CaRP image. The identified objects is used as cues to locate the points in password. Each password point has a tolerance range. A click within the tolerance range is acceptable as the password point. It is also resistant to Captcha relay attacks. CaRP can also help reduce spam emails sent from a Web email service.

4. Conclusion

In this paper we have seen about different types of Captcha and how they work. The application of the Captcha has also been discussed. In addition this paper explains different methods how Captcha can be created and how they are used for providing authentication. The discussed methods also explains how they are resistant to different kinds of attacks.

References

[1] Bin B. Zhu, Jeff Yan, Maowei Yang and Ning Xu, “Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems” IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014

[2] M. Alsaleh, M. Mannan, and P. C. van Oorschot, “Revisiting defenses against large-scale online password guessing attacks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012

[3] B. B. Zhu et al., “Attacks and design of image recognition CAPTCHAs,” in Proc. ACM CCS, 2010, pp. 187–200

[4] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, “A new CAPTCHA interface design for mobile devices,” in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8

[5] Sonia Chiasson, Robert Biddle, and Paul C., “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, March/April 2012

[6] Mun-Kyu Lee, “Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry”, IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014

[7] C. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on passpoints-style graphical passwords,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[8] M.Motoyama,D.McCoy,G.M. Voelker, and S. Savage, “Re: CAPTCHAs—Understanding CAPTCHA-Solving Services in an Economic Context,” in Proc. USENIX Security, 2010, pp. 435–452.

[9] L. 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. 1–9.

[10] Taekyoung Kwon, Sooyeon Shin and Sarang Na, “Covert Attentional Shoulder Surfing- Human Adversaries Are More Powerful Than Expected” IEEE Transactions On Systems, Man, And Cybernetics: Systems, Vol. 44, No. 6, June 2014.

[11] Napa Sae-Bae, Nasir Memon, Katherine Isbister, and Kowsar Ahmed, “Multitouch Gesture-Based Authentication” IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014

[12] Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha **“**Image Captcha Based Authentication Using Visual Cryptography” IJREAT , Volume 1, Issue 2, April-May, 2013

[13] Ved Prakash Singh, Preet Pal “Survey of Different Types of CAPTCHA” International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2242-2245

[14] Amalu James, Geo George,Asha Yeldose “A Survey on Spelling Based CAPTCHA” IJRCCT ,2014,ISSN(O) 2278-3814 ISSN(P) 2320-5186

[15] Beum Su Park1, Amlan Joyti Choudhury 1, Young sil Lee1, Tae Yong Kim “An efficient OTP Authentication Method using CAPTCHA” IEEE Transactions On Information Forensics And Security, Vol. 4, No. 6, April 2012

[16] Baljit Singh Saini and Anju Bala "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering, 2013, pp. 36-42, 2013.

[17] M. Chew and J. D. Tygar, “Image recognition captchas,” Tech. Rep. UCB/CSD-04-1333, EECS Department, University of California, Berkeley, Jun 2004.

[18] Greg Mori and Jitendra Malik. “Recognising Objects in Adversarial Clutter: Breaking a Visual CAPTCHA”, IEEE Conference on Computer Vision and Pattern Recognition (CVPR'03), Vol 1, June 2003, pp.134-141.

[19] J Yan and A S El Ahmad. “Is cheap labour behind the scene? - Low-cost automated attacks on Yahoo CAPTCHAs”, School of Computing Science Technical Report, Newcastle University, England. Apr, 2008.

[20] Chen-Chiung Hsieh and Zong-Yu Wu "Anti-SIFT Images Based CAPTCHA Using Versatile," IEEE, 2013.

[21] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.