ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

A New Multi-Panel Cartoon based CAPTCHA as Graphical Passwords

B.Santhosh Poornima[1], Dr.A.Padmapriya M.C.A., M.Phil, Ph.D[2]

Research Scholar, Department of Computer Science and Engg, Alagappa University, Karaikudi, India[1]

Assistant Professor, Department of Computer Science and Engg, Alagappa University, Karaikudi, India[2]

Abstract: Completely Automated Public Turning Test to tell Computers and Humans Apart (CAPTCHA) is essentially used to prevent some kind of malicious programs from accessing the web resource automatically. In modern era web services is an essential business tool in e-commerce. The emergence of intelligent, complicated attacks similar to DoS (Denial of Service) attack formulates web services still vulnerable. To moderate this attack, CAPTCHA is used as one of the most standard security technology. It is from uncomplicated ones, like typing the imprecise text also with differentiate an object in an image. In web security there is various kind of Captcha has been used to the purpose of security, such as text based Captcha, image supported Captcha, and audio oriented Captcha and video related captcha. This proposed paper indicates a novel online security scheme which is constructed with panel cartoons. Captcha is done with the turing test. Captcha as graphical passwords (CaRP) are incorporated and it generates a new family of cartoon based graphical password which is based on Jigsaw puzzle. The method proposed in this paper allows accessing the web services faster as well as in secured manner. The experimental results shows, the performance analysis in terms of security considerations by the combination of Captcha and graphical password scheme compared to existing methods.

Keywords: Satellite image, Image Encryption, Matrix form, Elementary Row Operations, Elementary Column Operation.

I. INTRODUCTION

With the advancement of Internet technology, Web security has grown to be a significant issue. There are a lot of numerous malicious threats across the web which produces the protection besides the system. Such kind of main threat is called Bot. A Bot is a malicious progression that has the ability to run automated responsibilities above the networks and construct a number of difficulties in the network. The present Internet infrastructure is susceptible to Denial of Service (DoS) attack [1]. For the reason that it depends on special consideration a huge amount of hosts to create traffic to an exacting destination, the harshness of DoS attacks increased as better facts of inadequately protected hosts which are linked to elevated bandwidth Internet connections. This will be diminishing the performance of the system. CAPTCHA is a well known security protection; it is used to protect these types of malicious programs [2].

Captcha is in various designs consist of text based or image based. In sequence to overcome the disadvantages of text based method, the image based captcha was initiated. Various internet web search engines like Yahoo, Google, and Bing etc to use captcha to distinguished among a authorized user and a malicious program [3].Captcha technique includes wide variety of applications such as the Website Registration Protection, shield against spam's and worms, avoiding comment spam's and avoiding the dictionary attacks. A Turing test was intended for establish the cleverness of a computer. The Turing test is the captcha series present as a judge and the other person act as user. When the user be failed the Turing test, consider to be a machine. Or else the user replicates to be a reliable user. To defend the online email and further services from being injured by bots, Captcha is a standard web application for protection practice [4]. In particular, the puzzle based panel cartoon has an extremely eminent conflict to attacks, security and simple to access. Furthermore, the evaluation cartoons is humorous and attractive for humans, the panel cartoon captcha inspiration is the popular feasible be seen as a pleasurable and enjoyable Turing test that does not harmfully have an effect on convenience for users. By using these category of captcha representation the user can simply access their submission by assemble this section within certain time duration. So among this progression the hackers cannot be able to attack the method during various injections. Jigsaw puzzle is a cartoon puzzle that mandatory a set of plenty mini and interlocking small images [5]. On completing the puzzle it generates a picture. The paper is designed as follows. Section 1 consists of the fundamental introduction about the captcha and basic security attacks. Section 2 highlights the related works on the captcha oriented security systems. Section 3 enclosed the proposed method for the captcha puzzle based panel cartoon. Section 4 demonstrates the results and discussions for the proposed method. Section 5 concludes the process with better performance.

II. RELATED WORKS

In 2015, Sandhya Rani et al.[6] has discussed a method, based on captchathat is a graphical passwords considered as a new security primitive which is dependent on unsolved Artificial Intelligence problems and hard Artificial Intelligence problems. The author describes the

DOI 10.17148/IJARCCE.2015.4785

captcha as a graphical password is both a graphical password technique and the captcha technique. A password of Captcha as graphical passwords can be found only probabilistically by automatic online guessing attacks that include brute force attacks, which cannot resist by other graphical password schemes lack. Hotspots in Captcha as graphical passwords images can no longer be exhibited to mount automatic online guessing attacks which are an inherent vulnerability in many graphical password systems. Captcha as graphical passwords forces adversary users to resort less efficient and Interactive attacks. In addition to offering security from guessing attacks made online, Captcha as graphical passwords is also resistant to Captcha relay attacks. Captcha as graphical passwords can also help reduce emails in spam sent from a Web email service.

In 2014, S. Karthika and Dr. P. Devaki. [7] Have proposed this paper about different types of Captcha and how they work. The author put forward it to, there are many Captcha techniques are design to provide better authentication for online application. It 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 an efficient Captcha technique to provide better authentication and protects the Captcha from different kinds of attacks using graphical password for Captcha. Thus this helps us to protect Captcha from attacks and also reduces the risk of providing low level authentication. The application of the Captcha has also been discussed in this paper. In addition to this paper it explains different methods how Captcha can be created and how they are used for providing authentication. The discussed method also explains how they are resistant to different kinds of attacks.

In 2014, Jayshree Ghorpade et al. [8] have proficiency put forward a survey for captcha graphical password security. In this paper the author conduct a comprehensive survey of existing CaRP techniques namely Click Text, Click Animal and Animal Grid. They discussed the strengths and limitations of each method and point out research direction in this area. The paper conducts a comprehensive survey of CAPTCHA as Graphical Password schemes. 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. The author has discussed Recognition-Based CaRP which include Click Text, Click Animal and Animal Grid techniques in this paper. They discussed current graphical password techniques are an alternative to text password butare still not fully secure. CaRP method works as a framework that does notrely on any specific CAPTCHA scheme. Converted schemes will continue in the place of destroyed one. Due to reasonable security and usability and practical applications, CaRP has good potential for refinements. The usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in.

In 2014, Bin B. Zhu et al. [9] proposed a new security based Artificial Intelligence problems with captcha protection. They have proposed CaRP, a new security primitive relying on unsolved hard problems of artificial intelligence. Their usability study of two CaRP schemes have implemented is encouraging. Animal Grid and Click Text methods are easier to use than Pass Points and a combination of text password and Captcha. Both Animal Grid and Click Text had better password exorability than the conventional text passwords. Different levels of images with difficulty can be considered for the process. CaRP utilizes unsolved Artificial Intelligence problems. Therefore there are more incentives for attackers to hack CaRP than Captcha. If attackers succeed, they contribute to improving artificial intelligence by providing solutions to open problems like segmenting 2D texts. Overall, their work is one step forward in the paradigm of using hard artificial intelligence problems for security.

In 2009 Haichang GAO Et Al. [10] explained to defend spyware attacks using a captcha. It is a program that generates and grades tests that are human solvable, but is beyond the capabilities of current computer programs. The author described captcha uses open algorithms based on hard AI problems, and has been discussed in text-based password schemes to resist dictionary attack. Innovatively, they explore CAPTCHA in the context of graphical passwords to provide better protection against spyware. As long as the underlying open AI problems are not solved, CAPTCHA is a promising way to resist spyware attack in graphical password schemes. Based on this key idea, the authors have proposed a new graphical password scheme using CAPTCHA, designed to be strongly resistant to spyware attack, either by purely automated software or via human participation.

III. PROPOSED METHODOLOGY

3.1 Captcha

The basic Captcha requires the user to type some alphanumeric characters specifically, alphabets or digits as of an imprecise image which is illustrated on the system display. The purpose of this kind of analysis is to avoid the unnecessary bots from accessing websites. In this proposed method, a security primitive based Captcha technology with graphical password system was presented to improve the online security. Its deal with an amount of security troubles altogether, for example, online guessing attacks, relay attacks and surfing attacks.

3.2 Proposed Technique

The methods used are:

- Know the working methodologies of Captcha
- Identify the functioning technique of Ajax
- Understand Jigsaw cartoon puzzle

DOI 10.17148/IJARCCE.2015.4785

This proposed method completely contributes a CAPTCHA by a panel cartoon. In this panel cartoon captcha, it is presented with the four panels rearranged or reshuffled randomly, the user was able to react with the particular order is recognized as a human. When the panels are rearranged randomly, the user knows the meaning of the picture and utterances all panels, and guessed the order it must be arranged to make a funny story. Random jumbled images are created by a captcha based Jigsaw model, which can be solved to generate the accurate cartoon which is arranged by drag and drop method. After each progress, the webpage will be automatically reloaded. It is easily accessed and it has lesser time.

The scheme illustrated in captcha challenge is applied, when the number of failed login attempts the threshold generated on the web account. A small threshold is applied for failed login attempts from unknown machines but a large threshold is applied for failed attempts from known machines on which a successful login occurred within a given time frame. This technique can be incorporated into CaRP (Captcha as graphical Password) to improve its usability:

1. A regular CaRP image is concerned when an account has accomplished a threshold of failed login attempts. As in, different thresholds are applied for logins from known and unknown machines.
2. Otherwise an "easy" CaRP image is applied. An "easy"

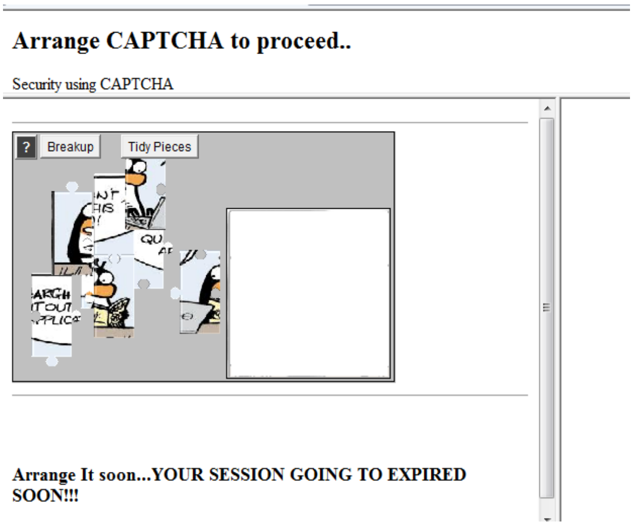
CaRP image may take several forms depending on the application requirements.

It may be an image provided by underlying Captcha generator with less distortion or overlapping, a permuted "keypad" wherein undistorted visual objects (e.g. characters) are permuted, or even a regular "keypad" wherein each visual object (e.g., character) is always located at a fixed position. These different forms of "easy" CaRP images allow a system to adjust the level of difficulty to fit its needs. With such a modified CaRP, a user would always enter a password on an image for both cases are listed as in above said and other extras are not required. Between the two cases difference lies in that a hard image is used in the first stage whereas an easy image is used in the second case.

IV.RESULTS AND DISCUSSIONS

The following results represent the working strategy of the proposed method. The given cartoon panel is initially rearranged, so that the interactive human has to arrange and proves their authentication. The cartoon panels should be arranged in proper manner within limited time duration. If the arranged sequence is the correct then the user is allowed to perform further process else otherwise the access is denied.

In the figure 1, the collapsed panels are provided along with session timings. Figure 2 reveals the original and sequences cartoon panel that has to be placed. Based on the proper replacement the user is allowed to sign in to their respective applications.

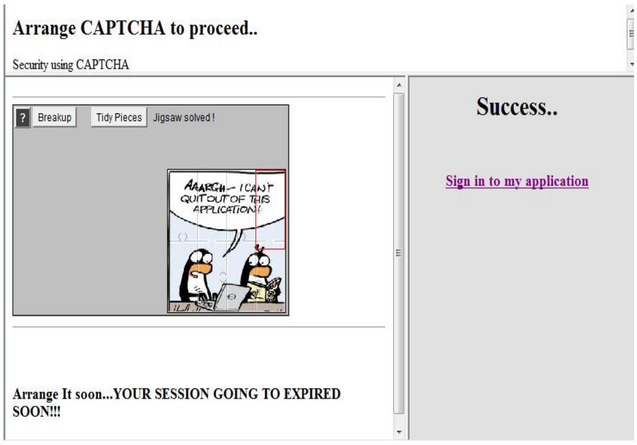


Arrange CAPTCHA to proceed..

Security using CAPTCHA

Arrange It soon...YOUR SESSION GOING TO EXPIRED SOON!!!

Figure 1 – Rearranged Cartoon panels as CAPTCHA



Arrange CAPTCHA to proceed..

Security using CAPTCHA

Arrange It soon...YOUR SESSION GOING TO EXPIRED SOON!!!

Success..

Sign in to my application

Figure 2 –Arranged Cartoon panels for CAPTCHA

V. CONCLUSION

Online security authentication is an important issue due to various attacks, so, captcha is a new security primitive technique relying on unsolved web service security problems. The proposed CaRP method is both a Captcha and a graphical password scheme. It is based on the panel cartoon puzzle. So when the user applies this technology, the keyboard is no need to solve the cartoon captcha. The captcha was assembled by drag the image by the use of mouse. The proposed approach is a user friendly approach for its easy access. This paper states a captcha Turing test with panel cartoons and the panel includes a cartoon based graphical password based on Jigsaw puzzle. The proposed method in this paper, gives better performance in terms of the security considerations, in addition to, the user with less intellectual can solve the test.

REFERENCES

[1] P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humans-in-the-loop,” ACM Trans. Inf.Syst. Security, vol. 9, no. 3, 2006, pp. 235–258.

[2] M. Alsaleh, M. Mannan et al, “Revisiting defenses against large-scale online password guessing attacks,” IEEE Trans. Dependable Secure Computer., vol. 9, no. 1, Feb.2012, pp. 128–141.

[3] H. S. Baird and K. Popat. “Human interactive proofs and document image analysis”,.Proc. of 5th IAPR Int. Workshop on Document Analysis Systems (DAS 2002), vol. 2423 of LNCS, 2002, pp. 507–518.

[4] Prof. Yogdhar Pandey, “Evaluating the Usability and Security of a Spelling Based Captcha System,” International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (3), 2014, pp. 4728-4731.

[5] T. S. Ravi Kiran, and Y. Rama Krishna, “Combining CAPTCHA and graphical passwords for user authentication”, International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012), ISSN 2231-4334.

[6] A. Sandhya Rani et al, “A New Security Primitive to Improve Security Using AI Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015, pp. 1086-1090.

[7] S. Karthika and Dr. P. Devaki, “An Efficient User Authentication using Captcha and Graphical Passwords-A Survey”, International Journal of Science and Research (IJSR), Volume 3, Issue 11, November 2014, pp. 852-855.

[8] JayshreeGhorpade et al, “Novel Method for Graphical Passwords using CAPTCHA”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4 Issue-5, November 2014, pp. 77-79.

[9] Bin B. Zhu et al, “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, pp. 891-904.

[10] HaichangGao et al, “A new graphical password scheme against spyware by using CAPTCHA”, Symposium on Usable Privacy and Security (SOUPS) 2009, July 2009, pp. 15-17.

[11] L. von Ahn, M. Blum, and J. Langford. “Telling Humans and Computer Apart Automatically”. Communications of the ACM, 2004, 47(2), pp.57-60.

DOI 10.17148/IJARCCE.2015.4785