CAPTCHA- to Enhance the Security in WWW

Asimkiran Dandapat
O.P.Jindal Institute of Technology, Raigarh, India 496 109

Arvind Singh Chandel
O.P.Jindal Institute of Technology, Raigarh, India 496 109

Gopal Singh Tandel
O.P.Jindal Institute of Technology, Raigarh, India 496 109

Abstract— In today's internet web security has become a challenging and critical issue. The internet BOT or web robot is one of the most spiteful threats to the web services. The WWW robot or simply BOT [1][8] is a software application that runs automated tasks over the internet and creates problem. One solution for securing web from BOT is to develop CAPTCHA [1][7]. CAPTCHA is acronym for Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHA may be in the form of text or image. In this paper discussion has been made on the available CAPTCHAs and a new way of image CAPTCHA has been proposed.

***Keywords*— CAPTCHA, BOT**

I. INTRODUCTION

CAPTCHA stands for Completely Automated Public Turing Test to Tell Computer and Human Apart that defends websites against BOTs by generating and grading tests that humans can pass but a computer program cannot. A corrupted text can be readable by Humans, but current computer programs can't. For many years, CAPTCHAs [2] have proven very useful for many reputable Web-based email and application service providers, online auction sites, social networking sites for the purpose of identifying automated registration. This technology is now almost a standard security technique for addressing undesirable or malicious Internet [2][3] programs (like spreading junk emails and grabbing thousands of free email accounts instantly) and has found widespread application on numerous commercial web sites including Microsoft MSN ,Google and Yahoo. It is accepted that a good CAPTCHA[7][8] must be usable and robust. The robustness of a CAPTCHA[4] is its strength in defending adversarial attacks, and this has attracted important attention in the research community.
There are the following three main types of CAPTCHAs:

1) Text-based schemes – These are typically rely on impure distortion of text images rendering them unrecognizable to the state of the art of pattern recognition programs but recognizable to human eyes.

2) Audio -based schemes- These are typically need the users to solve a speech recognition job.

3) Image-based schemes- These are typically require the users to recognize an image.

The main aim of a CAPTCHA is to resist form submissions from BOTs – automated scripts that get email addresses from the web forms. Many CAPTCHA's are very weak and that can be solved by cleaning the image and using simple OCR. Here are some examples CAPTCHA images in Fig 1.

Fig. 1 Different types of CAPTCHAs

CAPTCHA images can be passed by an OCR program to extract the text. In the Fig. 2 the distracting marks are lighter and the actual text is achieved.

Fig. 2 Parsed CAPTCHAs by program

Nowadays there are many software or browser add-ons are available that can finds any CAPTCHA on the web page, and it automatically send the CAPTCHA image to its own server, then any individual on the server machine reads the CAPTCHA image and sends back the characters shown in CAPTCHA to the client machine where the characters are inserted in the required textbox [7][8]. Hence by reading these we may conclude that CAPTCHAs are not trustworthy.

II. PROPOSED SCHEME

In order to enhance the security in web based applications, implementation of various types of CAPTCHAs on the client side in web application is proposed. Showing the drawbacks of Text CAPTCHAs & Audio CAPTCHAs implementation of Image-Recognition-Based CAPTCHAs is proposed. The Text-CAPTCHAs and Audio-CAPTCHAs can be cracked by various techniques like using OCR or any browser-add on softwares communicating with its server. But according to our proposed scheme we will implement Image-Recognition-Based CAPTCHAs in which we are going to display 8-10 different images showing different things and the positions of images will also change randomly each time they are used. The screen displaying the images will ask user to click on the particular image and this will continue for 4-5 times and if and only if all the clicks are made correct then he will be allowed to access the applications. Fig. 3 illustrates the Image Recognition Based CAPTCHA.

Fig. 3 Image Recognition Based CAPTCHA

III. IMPLEMENTATION

Most of the websites use the technique of CAPTCHA for validation / verification purpose whenever someone tries accomplish membership or want to submit a piece of information.

In most of the cases sometimes it happens that we need to have some [5][6]additional resources / dlls to be registered on the hosting server in order to implement the captcha basically this happens in case of server side scripting. Here we have implemented the CAPTCHA functionality purely on the client side using java technology.

IV. CONCLUSIONS

This proposed scheme is providing a new way of using CAPTCHA to obtain better security on web applications. There are also some types of CAPTCHAs like Text CAPTCHA, Audio CAPTCHAs etc. which have many drawbacks, this new technique will definitely overcome the drawbacks of CAPTCHAs. But due to frequent advancement in security domain we could not assure that the newly proposed scheme will remain secure forever. Therefore there is a huge scope to work on this scheme.

REFERENCES

[1] "A Framework to analyze the security of Text based CAPTCHA" by International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 27,2010.

[2] "Cryptographic Communication Using Natural Entropy" by Joseph Bonneau,University of Cambridge Computer Laboratory, June 2009.

[3] Nicholas J. Hopper, John Langford and Luis von Ahn. Provably Secure Steganog- raphy. In Advances in Cryptology, CRYPTO' 02, volume 2442 of Lecture Notes in Computer Science, pages 77-92. Santa Barbara, CA, 2002.

[4] M. Shirali-Shahreza and S. Shirali-Shahreza, "Collage CAPTCHA," Proc. IEEE Int'l Symp. Signal Processing and Applications (ISSPA 2007), February 2007.

[5] L. von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," Communications of the ACM, vol. 47, no. 2, pp. 57-60, February 2004.

[6] "Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA" by Greg Mori & Jitendra Malik, Computer Science Division, University of California, Berkeley.

[7] E. Bursztein, S. Bethard, J. C. Mitchell, D. Jurafsky, and C. Fabry. How good are humans at solving CAPTCHAs? a large scale evaluation. In IEEE S&P '10, 2010.

[8] J. Elson, J. R. Douceur, J. Howell, and J. Saul. Asirra: a CAPTCHA that exploits interest-aligned manual image categorization. In CCS '07, pages 366–374, New York, NY, USA, 2007. ACM.