International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 389-391
Published Online May 2020 in IJEAST (http://www.ijeast.com)

A SURVEY ON ENHANCEMENT OF CAPTCHA TO PREVENT NON INTERACTIVE ACCESS

Mr.Kumar K, Jyothipriya, Priyanka Pandit, Savinaya Shetty , Tejaswini G
Department of Computer Science and Engineering
K S Institute of Technology, Bangalore, India

Abstract - CAPTCHA is a Completely Automated Public Turing Test to tell Computers and Humans Apart, to ensure that the response is only generated by humans and not by computerized robots. Simpler CAPTCHAs are easily breakable due to advancement in pattern recognition and machine learning algorithms. There are enhancement procedures making few CAPTCHAs harder to decode. This paper brings the concept of human-friendly mini-game CAPTCHAs which is easier for the humans and difficult for the bots to break.

***Key Words*: bots; captcha; gamification; internet security; attacks; Turing tests, pattern recognition, machine learning algorithms.**

I. INTRODUCTION

CAPTCHA is abbreviated as Completely Automated Public Turing test to tell Computers and Humans Apart. It was developed in the year 2000 at Carnegie Mellon University by John Langford, Nicholas J. Hooper and Luis Von Ahn. CAPTCHA is used to differentiate between the humans and the computers. It prevents the system from spreading the viruses or vulnerable attacks. CAPTCHA is the verification test that can be found at the end of the sign-up page form in many websites. It is mainly used to protect services like surveys, polls, and registration forms. CAPTCHA should be easy enough and user-friendly to the user.

CAPTCHAs are a type of Artificial Intelligence. It cannot be solved by a computer system or by automated software; it is solvable only by a human being. The challenging task is to teach the computer about the human behavior and also to make the computer how the people think. The Artificial Intelligence has many algorithms, and it needs to be designed in such way that the computer behaves like a human, in order to explain the concept of CAPTCHA.

II. NEXT GENERATION GAME CAPTCHAs

The next generation game CAPTCHAs are based on human-friendly mini-games to tell computers and humans apart. These games are designed to using HTML5 and JavaScript and transmitted to the client browser in an encrypted form.

A. *Connecting Dots*

In Connecting Dots game the task may be given like connecting two red dots. The user needs to identify any two red dots in the CAPTCHA by clicking one dot and drag and drop to another red dot. This game is easy and human-friendly.

B. Drag-and-Drop

In Drag-and-Drop task is given, the user can drag and drop the object from one place to another place to complete the task. In the figure 9, there are three different shapes and there is also an empty space. To recognize a human, the user needs to fill the empty space by dragging the appropriate shape to the empty shapes. Once the user fills the shape, it will be authenticated; this is an another technique.

C. Duck Hunt

The Dunt hunt technique was followed, the user will see the ducks passing around, and the rule is, as given in the figure the user need to shoot three ducks, once the user shoots the ducks the CAPTCHA is verified, and the user was authenticated.

D. Bird Shooting

The bird shooting is an exciting game to click the flying birds to shoot and complete the task by shooting given the number of counts to determine the user is human. If robots are involved in this activity, it is easy to identify and prevent unauthorized activity to ensure the security of the website. In this below figure, there are different colors of birds are flying around, the rule given is to click the yellow bird, the user needs to click all the yellow birds in order to authenticate the correct user.

III. SECURITY ANALYSIS

The game based CAPTCHAs are purely developed and implemented using HTML5 and JavaScript. It will transmit to the client browser in the encrypted form, and intruders cannot able to decrypt the CAPTCHA code or hack the same.

A. *Random Guessing Attacks*

Here the CAPTCHAs a based on the mini-game, so the users need not provided any input to solve the same. There is no possibility of random guessing attack in next generation mini game CAPTCHAs. Random Guessing Attack is otherwise called as Brute force attack. Brute force attack is like trying with various combinations of letters, numbers, and symbols. As the combinations are correct, it works fine and the user can login and access resources

B. Dictionary Attacks

It is an authentication mechanism. The encrypted values are decrypted. The decrypted values are collected as a list. With the list of values, the user tries to guess a valid user's login and password. Once the user is valid, the system will allow accessing the resources.

IV. LITERATURE SURVEY

The paper [1] explains that the designing of captcha is as important as choosing captcha type. In this paper it's been showed that how color and design affects usability and security of captcha. In fact it is shown that how these factors can be utilized to improve captcha.

The paper [2] describes all types of captcha and also describes their drawbacks of all types of captcha. This also describes application of captcha. And review paper of different types of Captcha.

This paper [3] discusses usability issues that should be considered and addressed in the design of CAPTCHAs. Some of these issues are intuitive, but some others have subtle implications for robustness (or security).

The paper [4] shows the problems exist in present captcha system. We relate these flaws found in other CAPTCHA proposal. We conclude with some tips foe enhancing this CAPTCHA that can be considered as general guidelines.

This paper [5] examines CAPTCHAs and its working and literature Review. In registering websites, some intruders write malicious programs that waste the website resources by making automatic false enrolments that are called as bots. This paper also provides classification of CAPTCHAs, its application areas and guidelines for generating a captcha.

This paper [6] presents enhanced methods of generating captcha. According to this method An attacker can log on the test service system, only after he solves the moving object recognition problem. Such animation CAPTCHA will be able to resist the attacks of all the static OCR technology, and resist the mainstream of attacks against the moving object detection.

In this paper[7], we give a study case of the vulnerabilities in current login website using text-based CAPTCHA. Our target is a website of mainstream bank of china. We show that with some specialized methods, the CAPTCHA scheme in its website can be easily cracked. Finally, we give some advices for CAPTCHA designers to revise our CAPTCHA implementation security in the future.

In this paper[8] we will come to know usability, new techniques that have been used to change different CAPTCHA schemes, types of CAPTCHA. We than introduce the new level to solve CAPTCHA whether it would be in form of text, audio, image, video.

V. CONCLUSION

The proposed method ensures secure and interactive CAPTCHA. The proposed interactive method prevents non-interactive access. Using web scraping and OCR technologies the program can fetch the captcha data
and decode it. we then present a new defense system with enhanced CAPTCHA. which is the next
generation of CAPTCHA technology providing the first steps toward defending against CAPTCHA
attacks. We are trying to solve the problem by human-friendly method for quantifying the usability of
CAPTCHAs.

VI. REFERENCES

[1] Ved Prakash Singh, Preet Pal, (March 2014) "Survey of Different Types of CAPTCHA" in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2).

[2] .El Ahmad, A.S., Yan, J., Ng, W.Y.,(Sep 2012) "CAPTCHA design: Color, usability, and security". IEEE Internet Computing 16(2).

[3] Yan, J., Ahmad, A.S.E., (2008) "Usability of CAPTCHAs or usability issues in CAPTCHA design". In: Cranor, L.F. (ed.) SOUPS, ACM International Conference Proceeding Series, pp. 44–52.

[4] CJ Hernandez-Caston, A Ribagorda (May 2010) "Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study" computers & security.

[5] Baljit Singh Saini and Anju Bala (2013) "A Review of Bot Protection using CAPTCHA for Web Security," IOSR Journal of Computer Engineering.

[6] Xiao Ling-Zi and ZHANG Yi-Chun (2012) "A Case Study of Text-Based CAPTCHA Attacks," in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover.

[7] K Ling-Zi, X., & Yi-Chun, Z. (Feb 2012). *A Case Study of Text-Based CAPTCHA Attacks. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.*

[8] Bersha Kumari, Sarvesh Kumar, Jehangeer Ali Assistant Professor, Anita Kumawat, Hemant Gaur (2017) " Enhancing the Security of CAPTCHA based on the New Character Locations" published at 4th International Conference on "Computing for Sustainable Global Development

[9] Amrutha Pise, S.D. Ruikar (April 2014)

"Text Detection and Recongnition in Natural Scene Images" published at International Conference on Communication and Signal Processing.

[10] Walid Khalifa, Abdullah Hasan (June 2016) "A Survey on Current Research on Captcha"
Published in International Journal of Computer Science and Engineering Survey (IJCSES) Vol.7, No.3

[11] Rizwan Rahman (2012), "Survey on CAPTCHA systems" , journal of Global Research in computer Science, vol. 3, No.5.

[12] Ahn, L.Von. (2005) "Human computation" , Carnegie Melllon University, CMU-CS-05-19