IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 3, Ver. I (May. - June. 2018), PP 24-26
www.iosrjournals.org

Secured Conversion and Generation of Cognitive CAPTCHA Implementing Honeypot Technique

Divyashree N,
(Department of Computer Science, BMS College for Women/ Bangalore University, India)
Corresponding Author:Divyashree N,

***Abstract**: Internet has both brighter and darker side when it comes to information access. Authentication plays a major role in attempting authorized access to secured sections of web applications. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a security program used as non-reusable element for authentication purpose. Though there exist few robust CAPTCHA's like complex image CAPTCHA, iCAPTCHA and ReCAPTCHA they are to be used through CAPTCHA service provider(e.g.: Google) In some environments, a system is considered to be strong if the password is not transmitted to the verification process. This paper proposes two real-time authentication mechanisms namely cognitive CAPTCHA and honeypot generation for protecting the information being provided over internet.*

Date of Submission: 07-05-2018 Date of acceptance: 26-05-2018

I. Introduction

Authentication is a major field in security practice and research. Security is nothing but a program that completely avoids or reduces the risk of information protection. When it comes to information usage, internet plays in both positive and negative roles. Information theft, information destruction, website abuse for both sport and profit are some of the negative roles played using internet. Spammers employ web spams to increase traffic towards a website. The paper [1] describes various attacks on websites and techniques of protecting against it. The spam bots (or internet bots)[2,3] once programmed can be used several times for stealing user accounts and their information, for gaining access to secured information section, and for inserting spam contents(false contents) thereby making website vulnerable and unprotected.

Some of the motivations behind spam bots generation are:

1. Un-popularize a particular website.
2. Mislead of website user by redirecting them to view unsolicited contents.
3. To deceive ranks of websites over search engines.
4. Open several pages of the website thereby creating denial of service to actual users.

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is an automated security program used as non-reusable element for authentication. It is a smart intelligent program also can be called as an AI (Artificial Intelligent) program which identifies whether the legitimate user is a human or a robot. There already exist several CAPTCHA mechanisms [4, 5] as well as the CAPTCHA hacking techniques. Distinction between human and robot, making online poll more legitimate, safe browsing and online shopping, removal of abuse contents are some of the advantages of implementing CAPTCHA system. There are few disadvantages associated namely reduction in revenue from the website, illegible CAPTCHA's that are great difficult for even humans to understand, prevention of spam bots completely. The paper [6] presents the importance of human cognitive factor in building various CAPTCHA techniques like Mathematical, Analytical, image, etc. Thought there are many robust CAPTCHA techniques like complex iCAPTCHA, ReCAPTCHA(by Google), Ajax fancy CAPTCHA etc. , they are not incorporated by many websites due to lightweight requirement of websites, size of their websites, as well as unnecessary requirement of relying on CAPTCHA service provider. The paper [7] provides information of various CAPTCHA breaking tools. Web spam bots usually tries to hack CAPTCHA (basic CAPTCHA) if implemented and auto fills the form fields of the website to gain legitimate access.

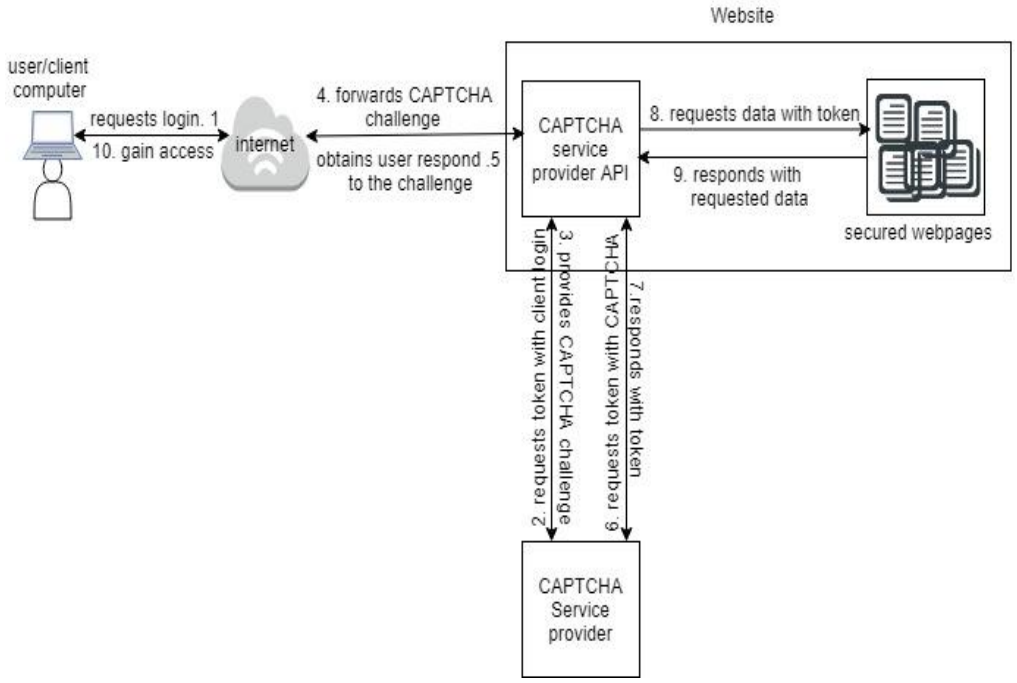

Figure1: CAPTCHA implementation through CAPTCHA service provider

The above figure explains how actually the CAPTCHA system is implemented by a website where in for every user request to access secured information, the webpage will be redirected to CAPTCHA service provider site for authentication using CAPTCHA.

The next desired technique apart from CAPTCHA is the Honeypot technique [8,9] to trap spam bots from illegal access. The paper [10] work describes three different tags to find whether a URL is clocked or not.

There are several ways to implement honeypot technique in the webpage code.

1. Make input type hidden
2. Make CSS position absolute
3. Set CSS display property to none
4. Set CSS visibility property to hidden or collapse
5. Set CSS opacity to zero
6. Indenting text to 100%
7. Use JavaScript or jQuery to put honeypot code.
8. Use sematic traps

Instead of using service provider's CAPTCHA for security purpose, why not have our own simple yet robust CAPTCHA generation system combined with an intelligent honeypot technique to tackle spam bots?. This paper proposes a secured way of cognitive based CAPTCHA generation and combining honeypot technique without any complexity.

II. Generation of Cognitive CAPTCHA

The CAPTCHA generation technique has been designed to generate a mathematical CAPTCHA (Even a simple text CAPTCHA can be generated) and instantly convert it into an image and prompt the user to solve it. Though there are many CAPTCHA breaking tools for reading image contents like OCR (optical code reader), they are not intelligent enough to solve a cognitive based CAPTCHA (Mathematical CAPTCHA). The important factor here is the generation of cognitive CAPTCHA as a non-reusable element within the webpage itself rather than relying on CAPTCHA service provider, building codes and URL's to connect to the service provider for authentication.

III. Honeypot Implementation

As described honeypot is a smart trap code to fish out the spam bots. Honeypot is a tricky code which expects nothing from the legitimate user and traps only the spam bots. All that is required to implement a honeypot technique is to add hidden form fields in CSS (Cascading Style Sheet) or in jQuery (JavaScript) as the spam bots often don't see the difference between visible and invisible fields.

IV. Proposed System Model

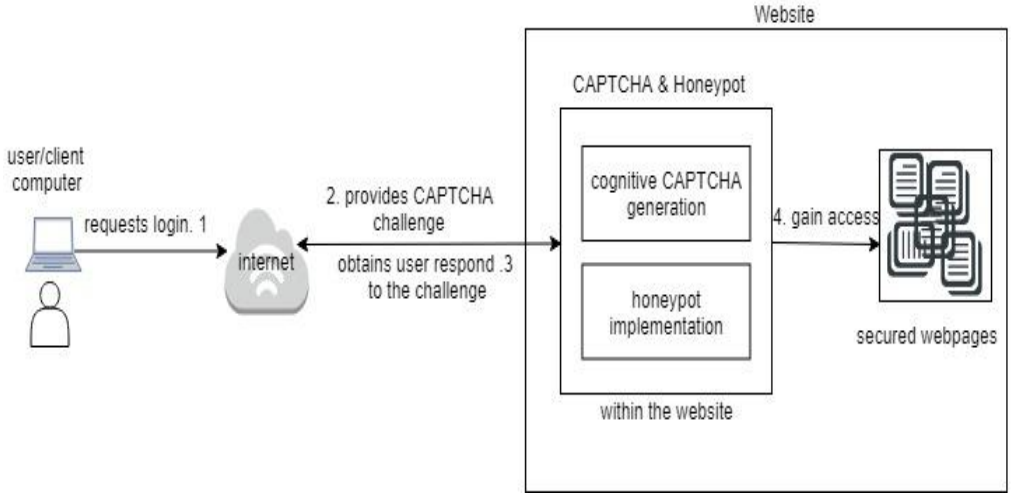

Figure 2: Proposed System Model

Figure 2 explains about the proposed system model where cognitive CAPTCHA generation and Honeypot code is embedded within the website itself. Here the idea is to trap spam bots in two ways: one way through enhanced CAPTCHA where bots might break the image molded cognitive CAPTCHA but fail to solve it and the other way is to trick and trap them through Honeypot technique.

V. Results

The performance of a website depends on user side and server side factors. Some of the user side factors are download speed, browser, cache memory and processor speed. Factors from server side include website load time, file types, webserver capacity and scripts. Performances from users point of view various depending on the type of system (PC or laptop) that the user is using. Thereby ignoring the user side factor, the performance can be measured only from server side. I have used GTmetrix tool to analyze the website performance with the inclusion of cognitive CAPTCHA-honeypot code within the website and with the use of service provider CAPTHCA. It is observed that the response time of the website is faster with the cognitive CAPTCHA-honeypot code which is built within the website than the one which uses other CAPTCHA service provider.

VI. Conclusion

Cognitive CAPTCHA is designed mainly for having legitimate user access and conversion of it to image in real-time and implementing a honeypot trap gives a deviation for the spam bots to get trapped there by eliminating the robot spams. Since honeypot and cognitive CAPTCHA are generated in real-time within the website, risks of relying on CAPTCHA service providers, facing denial of services and bearing its cost are completely eliminated.

References

[1]. Chris Mitchell, threat Researcher "Securing Websites" A SophpsLabs technical paper, SophosLabs UK, 2011
[2]. SumitSahu, BhartiDongre, Rajesh Vadhwani "Web Spam Detection Using Different Features" International Journal of Soft Computing and Engineering (IJSCE), Volume-1, Issue-3, July 2011
[3]. Dinie Florencio and Cormac Herley Microsoft Research, "Entering Passwords on a Spyware Infected MachineDinei" (textbook)
[4]. Vedprakash Singh, Preet Pal "Survey of Different Types of Captcha" International Journal of Computer Science and Information technologies, Vol. 5(2), 2014,2242-2245
[5]. Divyashree N, Dr.T.Satish Kumar "Survey on Captcha Categories" International Journal Of Engineering and Computer Science. Vol 5 issue 5 May 2016,ISSN:2319-7242
[6]. Mohammad JabedMorshedChowdhury, Narayan RanjanChakraborty" CAPTCHA based on Human Cognitive Factor" International Journal of Advanced Computer Science and Applications, Vol 4, No. 11, 2013
[7]. Shujun Li, Syed AmierHaider Shah, Muhammad AsadUsman Khan, Syed Ali Khayam, Ahmad-Reza Sadeghi, Roland Schmitz "Breakign e-Banking CAPTHCA's" Preceedings of 26th Annual Computer Security Application Conference, Dec. 6-10, 2010 Austin, Texas, NewYork, NY:ACM, 2010 pp.171-180
[8]. http://haacked.com/archive/2007/09/11/honey-pot-captcha.aspx/
[9]. https://jennamobly.com/
[10]. Jun-Lin "Detection of clocked web spam by using tag-based methods" Expert systems with Applications 36(2009) 7493-7499

Divyashree N "Secured Conversion and Generation of Cognitive Catch Implementing Honey pot Technique." IOSR Journal of Computer Engineering (IOSR-JCE) 20.3 (2018): 24-26.