International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Hypothesis on Approach which Distinguishes Soul from Automaton

Vinay J Uttekar[1], Ranjit P Lawale[2]

MCA Department, Bharati Vidyapeeth's Institute of Management and Information Technology

Abstract: ***CAPTCHA is a technique to distinguish human from bots, a way of thwarting spam and automated extraction of data from websites [1]. This paper discuss the various techniques to implement the CAPTCHA system. The paper also discuss various ways to penetrate available CAPTCHA system on internet.***

Keywords: Advanced Risk Analysis, CAPTCHA, Control Word, noCaptcha, reCaptcha, Unknown Word

1. Introduction

CAPTCHA is a computer program or sys-tem intended to distinguish human from machine input, typically as a way of thwarting spam and automated extraction of data from websites [1]. The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University [2]. There are various techniques available on internet which distinguishes between human and automated programs. This paper gives the review of these techniques. It also discuss various ways to penetrate available CAPTCHA systems.

2. Literature Review

From the research on internet, we found vari-ous techniques which implements CAPTCHA system in different ways. reCaptcha, no-Captcha techniques are reviewed in this paper. reCaptcha is armed with its state of art of algorithms which itself evolves and learns which is known as machine learning. reCaptcha advances with 2 level security by adding two words namely unknown word (difficult to identify) and control word(easy to identify) to its captcha in order to prevent spam and differentiate bots from human. Unknown words are failed to be identified by OCR scanners. It is widely used for preventing database related attacks like SQL injection. It also prevents the network flooding attack by bot scripts. On average 10 seconds of human effort time wasted. So, reCaptcha version 2 is introduced.

No Captcha reCaptcha is new version 2 of reCaptcha, where a single checkbox next to the statement "I'm not a robot" gets you where you want to go to identify user from bot [3]. It uses a sophisticated backend analysis called Advanced Risk Analysis to consider the users engagement before, during and after clicking the checkbox while identify the users. It uses some known factors which include users IP ad-dress, browser cookies, and even mouse move-ment to identify user from bots.

From the above discussion it is conclude that we have simple noCaptcha reCaptcha tech-nique which is widely used to stop spam and automatic extraction of information.

3. Application

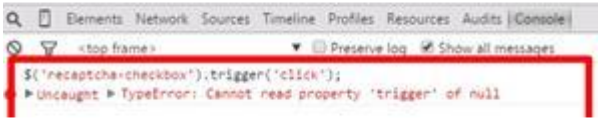
By reviewing the above techniques, it is clear that noCaptcha reCaptcha is simple choice. The application is to penetrate noCaptcha re-Captcha technique. To do so, we have used various external tools.

According to google, noCaptcha reCaptcha is just a checkbox that user need to tick.

In penetration test, we wrote jquery script, a javascript library, to triggerclick event on checkbox. We went to official reCaptcha demo link by google, (www.google.com/recaptcha/api2/demo).

We turn on inspect element by F12 key and note down the check box class i.e. recaptcha-checkbox. Now in the console we wrote an jQuery command to trigger an click event to that checkbox. Command we used was, $('.recaptcha-checkbox').trigger('click'); After this test, we found jQuery trigger event failed in console with reporting an error saying, Cannot read property 'trigger' of null.

Following image shows the sample of captcha.



```
$('recaptcha-checkbox').trigger('click');
▶Uncaught ▶TypeError: Cannot read property 'trigger' of null
```

Figure 1: jQuery Test

By further investigation we found that, when user clicks on checkbox, one request is sent to google API. In return, API provides one token which get stored in hidden field named 'g-recaptcha-response'. We tried 'reply' attack. We saved token returned for first request. Then, on next request, we initialized hidden field named 'g-recaptcha-response' with previously saved value. When we tried to save form without ticking the checkbox. Form return error saying, "invalid captcha".

For penetration test, we used HP QuickTest Professional [4]. It provides functional and regression test automation for software applications and environments [4]. We created new automated test case. Started recording, in web application we added ”www.google.com/recaptcha/api2/demo”.

We clicked checkbox, and then pressed submit button. We stopped recording. When, we tried to run this recording, we found that, click movement was not captured by HP QuickTest Professional [4].

4. Conclusion

This paper briefly reviewed various implemen-tation of CAPTCHA system. Also, we ran penetration test on noCaptcha reCaptcha technique. We will be able to eventually save thousands of hours per day of mankind. reCaptcha version 2 passes through the penetration testing and bots could not trigger any event, automation failed, replay attack was not successful. So, noCaptcha reCaptcha claim of Google was found to be ’true’.

References

[1] https://www.google.co.in/search?q=CAPTCHA
[2] http://www.captcha.net/
[3] https://www.google.com/recaptcha/intro/invisible.html
[4] https://en.wikipedia.org/wiki/HPQuickTest Professional