ISSN:0975-9646

Yogdhar Pandey et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4728-4731

Evaluating the Usability and Security of a Spelling Based Captcha System

Prof. Yogdhar Pandey
Sagar Institute of Research & Technology
RGPV University Bhopal ,India

Darshika Lothe,
M.Tech in software Engineering
Sagar Institute of Research & Technology
RGPV University Bhopal, India

Abstract - In this CAPTCHA system named Clickspell has been widely used for preventing malicious programs to access web resources automatically. In this paper, a new type CAPTCHA system will be proposed. The proposed scheme, named Clickspell, combined the features of text-based and image-based CAPTCHAs. Click spell, tries to increase each security and usefulness of CAPTCHA, Clickspell asks users to spell a randomly chosen word by clicking letters for passing the test all the letters are distorted. Users can learn the definition(s) of the chosen word which is display on CAPTCH image . In addition, Clickspell can add an advertisement image optionally. Clickspell improved the capability of resistance to the attack by malicious programs. Our preliminary test showed that Clickspell is practical in the aspects of security and usability.

Keywords: **CAPTCHA; Information Security; User usability; Clickspell; Optical Character Recognition(OCR); Internet Security; Image Processing;**

I.INTRODUCTION

Web Services are major applications provided on the Internet. These Web Services include free e-mail accounts, chat rooms, discussion board, blogs, on-line booking, and so on. Along with the Web Services, there is an essential issue that is how to avoid the massive and automated access to Web resources through malicious robots (automated program). For example, if the server did not provide suitable mechanism to prevent the robots. The CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) is a system, widely is used on the web to avoid various malicious robots to abuse the network resources. A good CAPTCHA system must satisfy the following three characters: (1) Human can recognize the contents and pass it easily. (2) It is invoked to prevent robots to pass the system or to increase the processing cost through continuous attack. (3) It should be generated easily and quickly. In recent years, there are many types of CAPTCHA system have been explored. All of the research results can be categorized into four types: Text-based, Image-based, Audio-based.

TEXT BASED CAPTCHA

Text-based CAPTCHA asks users to recognize the word, that has been presented in a distortion form. This type of CAPTCHA is intuitive to users. In other words, it is easy to use without learning or training. Text-based CAPTCHA is most widely deployed in many famous websites, eg. , Yahoo, Hotmail, Gmail, YouTube, PayPal and so on. It shows a synthetic handwritten word, which uses pre-existing character images to generate cursive English handwritten text line for blocking robots.

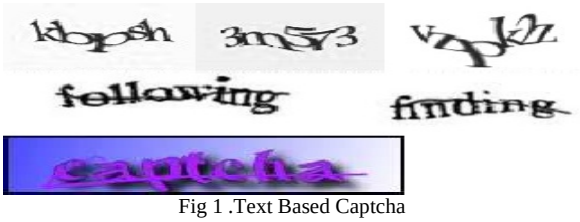

Fig 1 .Text Based Captcha

IMAGE-BASED CAPTCHA

In image-based CAPTCHAs, users have to identify the subject of an image. This type of CAPTCHA usually interacts with users by using a pointing device, e.g., mouse. In general, image-based CAPTCHAs require larger web page area, and need an image database maintained at the server.

Fig 2. Image Based Captcha

AUDIO-BASED CAPTCHA

Audio-based CAPTCHAs ask users to recognize the vocabulary that is heard from a speech. In general, an audio based CAPTCHA includes three parts: vocabulary,

noise and audio production. To prevent robots from attacking easily, noises should be added into the speech. In addition, these noises should be created dynamically to increase the difficulty of recognition by robots. The audio-based CAPTCHA is an alternative for visually-impaired people.

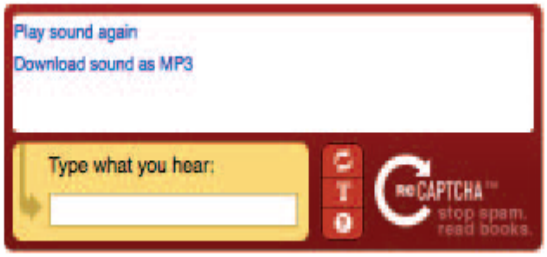

Fig 3. Audio Based Captcha

.

II. PROBLEM SYSTEM DEFINATION

Clickspell CAPTCHA:

The CAPTCHA image of Clickspell can be divided into four parts: Banner area, explanation area, click area and advertisement image. Each part performs a particular function as follows.

Banner area:

Display a word randomly chosen from the English dictionary. And this word is used for testing users. The users have to spell it by clicking the letter by letter for passing the test.

Explanation area:

Show the meaning of the chosen word in the designated language. This function utilizes Google dictionary. And there are more than 40 different languages that can be used. Users can read the word definition and its examples by clicking the explanation area. Furthermore, to click the sound icon will pronounce the word.

Click area:

All the letters of the testing word are properly distorted and randomly located in the click area. In the click area, a background image is placed under the letters. In order to against the robots' attack, the background image is generated by drawing lines, dots, polygons with random colors and sizes.

Advertisement image:

Click area can be covered an image and the covered image could be an advertisement.

Fig.4 an advertisement image is placed on the top of click area and accompanying added a circle mask Users can move the mask to finding the letters .

III. SYSTEM FEATURES

Preventing Comment Spam in Blogs

Most bloggers are familiar with programs that submit bogus comments, usually for the purpose of raising search engine ranks of some website (e.g., "buy penny stocks here"). This is called comment spam. By using a CAPTCHA, only humans can enter comments on a blog. There is no need to make users sign up before they enter a comment, and no legitimate comments are ever lost!

Protecting Website Registration

Several companies (Yahoo!, Microsoft, etc.) offer free email services. Up until a few years ago, most of these services suffered from a specific type of attack: "bots" that would sign up for thousands of email accounts every minute .The solution to this problem was to use CAPTCHAs to ensure that only humans obtain free accounts. In general, free services should be protected with a CAPTCHA in order to prevent abuse by automated scripts.

Protecting Email Addresses From Scrapers

Spammers crawl the Web in search of email addresses posted in clear text. CAPTCHAs provide an effective mechanism to hide your email address from Web scrapers. The idea is to require users to solve a CAPTCHA before showing your email address.

Online Polls

As is the case with most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Mellon found a way to stuff the ballots using programs that voted for CMU thousands of times. CMU's score started growing rapidly. The next day, students at MIT wrote their own program and the poll became a contest between voting "bots." MIT finished with 21,156 votes, Carnegie Mellon with 21,032 and every other school with less than 1,000. Can the result of any online poll be trusted? Not unless the poll ensures that only humans can vote.

Preventing Dictionary Attacks

CAPTCHAs can also be used to prevent dictionary attacks in password systems. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins. This is better than the classic approach of locking an account after a sequence of unsuccessful logins, since doing so allows an attacker to lock accounts at will.

Search Engine Bots

It is sometimes desirable to keep web pages un indexed to prevent others from finding them easily. There is an html tag to prevent search engine bots from reading web pages. The tag, however, doesn't guarantee that bots won't read a web page ;it only serves to say "no bots, please." Search engine bots, since they usually belong to large companies, respect web pages that don't want to allow them in. However, in order to truly guarantee that bots won't enter a web site, CAPTCHAs are needed.

III. HOW THE PROPOSED SYSTEM WORK

Step 1:

Randomly chooses a word, *W*, from English dictionary (stored in a database). And place *W*on the banner area. Let |*W*| denotes the number of letters of *W*.

Step 2:

Set the click area of size *CW* ×*CH* pixels. Produce the background image by drawing lines, dots, and polygons with random colours, transparencies and sizes. The number of the drawing objects depends on the size of *CW* ×*CH*. The larger size of *CW* ×*CH*, the number of drawing objects must be increased. For example, the number of dots equals *CW*×*CH* 20 , the of polygons is equals *CW*×*CH* 2500 , the count of oblique lines equals*CH*100 + 5 and the amount of horizontal lines equals*CW*200 + 5 in Figure (a). Note that all the numbers ofthe drawing objects are derived from the experimental results.

(a) javascript, 300 × 300.

Step 3:

Set the letter of size *LW* × *LH* pixels. Each latter *Li* ∈*W,* for *i* = 1, 2, . . . ,|*W*|, is properly distorted and randomly placed in the click area (above the background image). Note that in the click area, *Li* cannot overlap with *Lj*, where *j* _= *i,* 1 ≤ *i, j* ≤ |*W*|.

Step 4:

Get the definitions and examples of *W* from the web service of Google dictionary with URL parameters. The parameters include source language, target language, and query word *W*. For example gd&sl=en&tl=zh-TW&q=assist will receive the definition and examples of the query word 'assist' in JSON (JavaScript Object Notation) format. Here the source language is English and target language is Traditional Chinese. After receive all of the definitions and examples of *W*, place the

first definition of *W* on the explanation area. And put all the definitions and examples of *W* into the pop-up window.

Step 5:

If necessary, places the advertisement image of size *CW* ×*CH* on the click area. When the advertisement image is placed, a circle mask is put on the advertisement image for looking for the letter *Li* ∈*W*. The centre of circle mask is bound to the position of pointer device, e.g. Mouse. User can move the pointer device to look and click the letters for spelling the test word *W*.

Note that in Step 3, the letter size of *LW* × *LH* for each *Li* is not limiting the same. In other words, each *Li* can be assigned a different size of *LW* × *LH*. On Clickspell system, users will pass the test by spelling *W* correctly. While during the spelling process, the user may click a wrong letter. If the click errors greater than Emax , the test is fail. For Example, *Emax*= 2 means that the test is failure when the third click error occurs

.

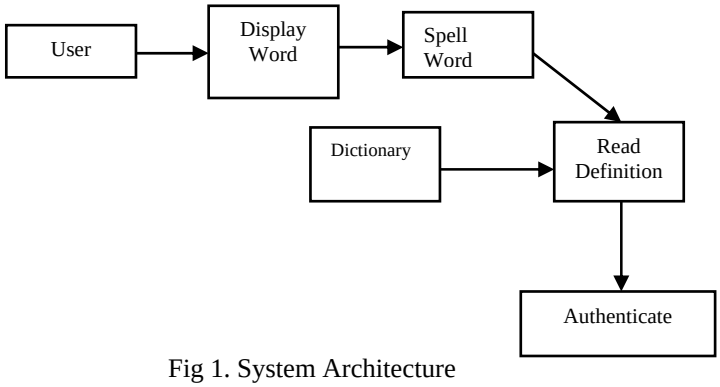

Fig 1. System Architecture

IV. ADVANTAGES

Human can recognize the contents and pass it easily. It is invoked to prevent robots to pass the system or to increase the processing cost (e.g. time) through continuous attack. It should be generated easily and quickly.

Security: To resist the attack of malicious programs.

Usability: To increase the rate of passing the test.

Extensibility: To provide a dictionary function for users to learn about the meaning and the spelling of words. In addition, an advertisement can be placed on the top of CAPTCHA images.

V. SECURITY REQUIREMENT

Administrator has all privileges of system. After the CAPTCHA expires, he cannot submit the conformation form. Each User is assigned different CAPTCHA when expired time limit.

VI. CONCLUSION

To pass the Clickspell test, users have to spell a randomly chosen word by clicking on distorted letters. Clickspell derived the main feature of text-based CAPTCHA, i.e., easy to use. Furthermore, Clickspell retains the character of image-based CAPTCHA, i.e. recognize objects from an image. Clickspell provides the dictionary function for users to learn the definition(s) of the spelling words. Furthermore Clickspell can add an advertisement image optionally. Because of the advertisement image covered the distorted letters, malicious programs are harder to attack Clickspell. The experimental results showed that the distorted letters cannot be segmented and recognized by several OCR tools. In additions, the investigated results showed that the mean click error rate is less than 3% and the mean pass rate is larger than 98%in 7.62 seconds. Consequently, Clickspell is practical when considering the aspects of security and usability. In particular, Clickspell is suitable for the devices which without a keyboard, e.g., smart phone, tablet PC and so on

ACKNOWLEDGMENT

This research would not have been feasible without encouragement and guidance of *Prof. Yogdhar Pandey* . He patiently discussed ideas with me and gave suggestion.

We are grateful to Head Of Computer Department, Sagar Institute of research and Technology, Bhopal and Research for always being ready to help with most diverse problem that we have encountered along the way.

We express our sincere thanks to all staff and colleagues who have helped us directly or indirectly in completing this paper.

REFERENCES

[1] R. Datta, J. Li, and J. Z. Wang, "Imagination: A robust image-based CAPTCHA generation system," in Proc. ACM Multimedia, Singapore, 2005, pp. 331–334

[2] Y. Ariki, S. Mizuta, M. Nagata, and T.Sakai. Spoken word recognition using dynamic features analysed by Two dimensional cepstrum. In Communications,Speech and Vision, IEE Proceedings I, volume 136, pages 133–140.IET, 2005.

[3] B. Boashash. Time frequency signalanalysis and processing : a comprehensivereference / edited by Boualem Boashash. Elsevier, Amsterdam ; Boston 2003.

[4] E. Bursztein and S. Bethard. Decaptcha:breaking 75% of eBay audio CAPTCHAs.In Proceedings of the 3rd USENIX conference on Offensive technologies, page 8. USENIX Association, 2009.

[5] E. Bursztein, S. Bethard, C. Fabry, J.Mitchell, and D. Jurafsky. How good arehumans at solving CAPTCHAs? a largescale evaluation. In Security and Privacy(SP), 2010 IEEE Symposium on, pages 399–413. IEEE, 2010.

[6] K. Chellapilla and P. Simard. Usingmachine learning

[7] M. Blum, L. Von Ahn, J. Langford, and N. Hopper, "The CAPTCHA Project, Completely Automatic Public Turing Test to tell Computers and Humans Apart," Dept. of ComputerScience, Carnegie-Mellon Univ., http://www. captcha. net.

[8] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA," IEEE Conference on Computer Vision and Pattern Recognition, vol. 1, pp. 134–1412003.