IJCSMA

S.Thangavelu *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 6, June- 2015, pg. 37-43 ISSN: 2321-8363

Security and Usability Issues in Captcha Design

S.Thangavelu[1]; T.Purusothaman[2]

[1]M. S. University, Tirunelveli, India, E-mail: s_thangavelu@rediff.com
[2]Govt. College of Technology, Coimbatore, India

DOI: 10.47760/ijcsma.2015.v03i06.001

Abstract

Captcha stands for Completely Automated Public Turing test to tell Computers and Humans Apart. Captcha is a challenge response test which determines whether the user on Internet is human or a spam robot. They are also called as Human interactive proof. Captcha is used to prevent the automated attacks by the computer robots. The Captcha test generates a simple task which can be easily solved by humans and hard for bots to complete the task. Thus Captcha prevents the unauthorized entry of bots into the websites and web services.

Keywords: Captcha, bots, security, usability, Internet.

1. Introduction

Internet has opened a modern world for the people. The Internet connects people; it is a source of information, a social platform, and a business network. Internet based activities like online education, email, online ticket bookings, net banking and online shopping etc., become possible for the humans within few seconds. The amazing growth of the Internet also suffers by spamming, scraping and other malicious attacks by automated computer bots. A bot short for robot is computer software that automates a task. In general the bots are used to do some repetitive tasks and they can do them, much faster than humans. Bots can be mostly used for productive tasks but frequently used for malicious purpose also. The malicious bot programs impersonate like a human and access the web services created for humans. They perform malicious activities in the online services and create lot of problems by breaching the web security. Hence a security method needed which ensures the presence of humans in the web services. Captcha [1] is one of the most powerful security method employed in all popular websites.

2. Different Types of Captcha methods and Bots

Captcha is an automated test which asks the users to identify some letters, numerals, images, audio and videos. The letters are distorted and presented in a noisy background so that bots cannot identify them easily. In order to pass the Captcha test the human users need to interpret the distorted text and type the correct letters in the text box and submit for authentication. If the input characters match with the Captcha characters then permission will be granted to access the web services. This is a robust challenge for the bot programs. Bots are present all over the Internet used for both the legitimate and malicious purposes. Good bots are known as legitimate bots, which perform beneficial actions to the website and the bad bots are called as malicious bots[2] which perform malicious actions, they are,

- **Spam Bots:** The main purpose of spam bots is to collect the email addresses for spamming. These bots spiders on the Internet web pages and collect data from forms that have been filled out online, posting advertisements and pop ups all over the Internet.

- **Hacker Bots**: Online Hackers use this type of bots to crawl around the Internet and to find all contacts in websites and online applications. They can be utilized for malicious purposes.

- **Spy bots:** It is also known as surveillance or data mining bots. Spy bots are used to collect data and information about an individual, website or organizations for malicious activities.

- **Download Bots**: These are bots that are used to compulsorily download a web page that the hacker wants the user to see instead of a web page that the user requested.

Captcha security methods [3] can be broadly classified as,

- Text based Captcha
- Image based Captcha
- Captcha based on audio
- Captcha based on video

The text based Captcha methods are very easy to implement and user friendly. It consists of random alphabetic or alphanumeric characters presented with distortion and added noise to the user. The text based Captcha methods also incorporated with waved characters, 3D characters, rotated characters, scattered characters to confuse the Internet bots. Figure.1. shows the text Captcha images [4] with blurring, waving, tilting effects. Figure.2. shows the text based Captcha images used in the popular email services such as Outlook Email, yahoo Email, AOL Email, Rediff Email and Hotmail.

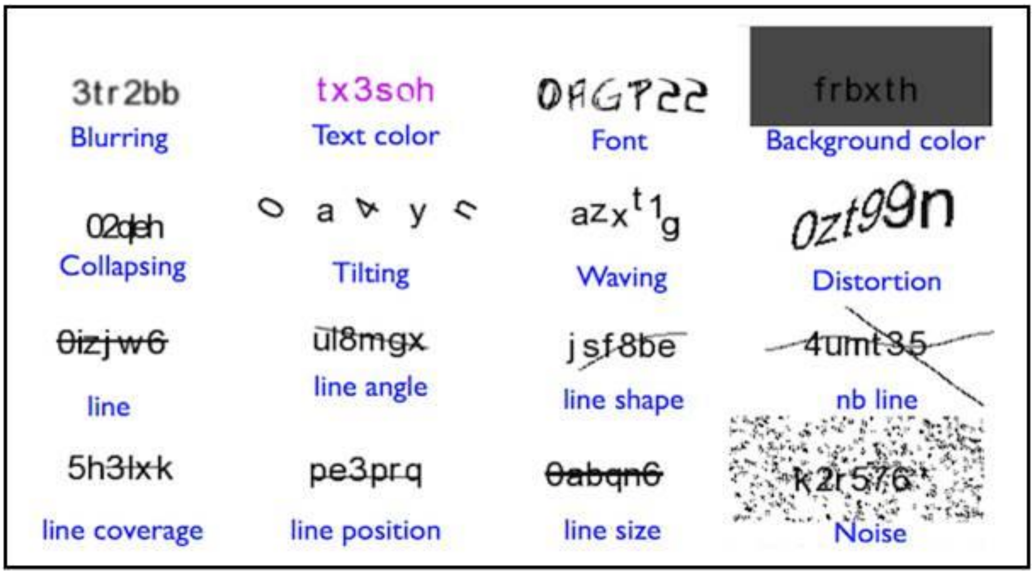


Figure.1. Text Captcha images with blurring, waving and tilting effects

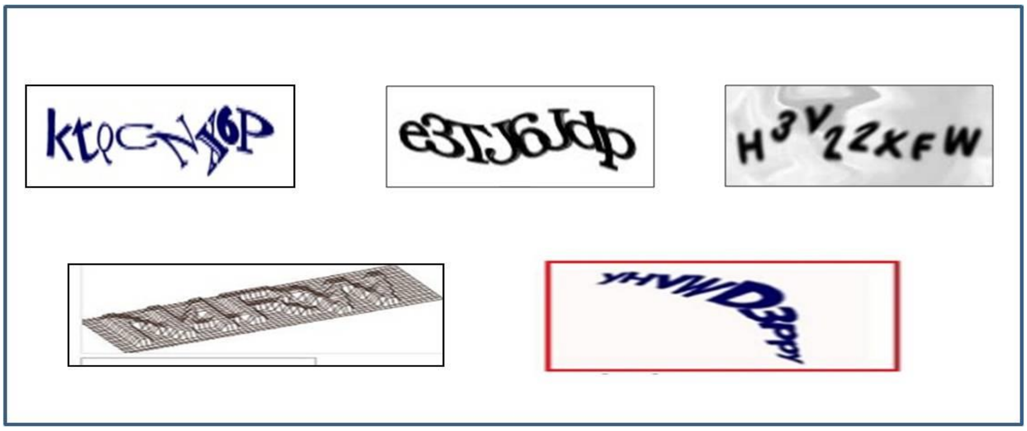


Figure.2. Text based Captcha images used in the popular Email services

The Image based Captcha methods [5] are designed by using various image objects and patterns. The user has to identify a specific image to pass the test. Sometime the users need to perform image matching, face matching and pattern matching to prove him as human user. Figure.3. shows the various image based Captcha methods. This Captcha is difficult for some users having low vision and color blindness. The image based Captcha methods are also suffered by various automated attacks.

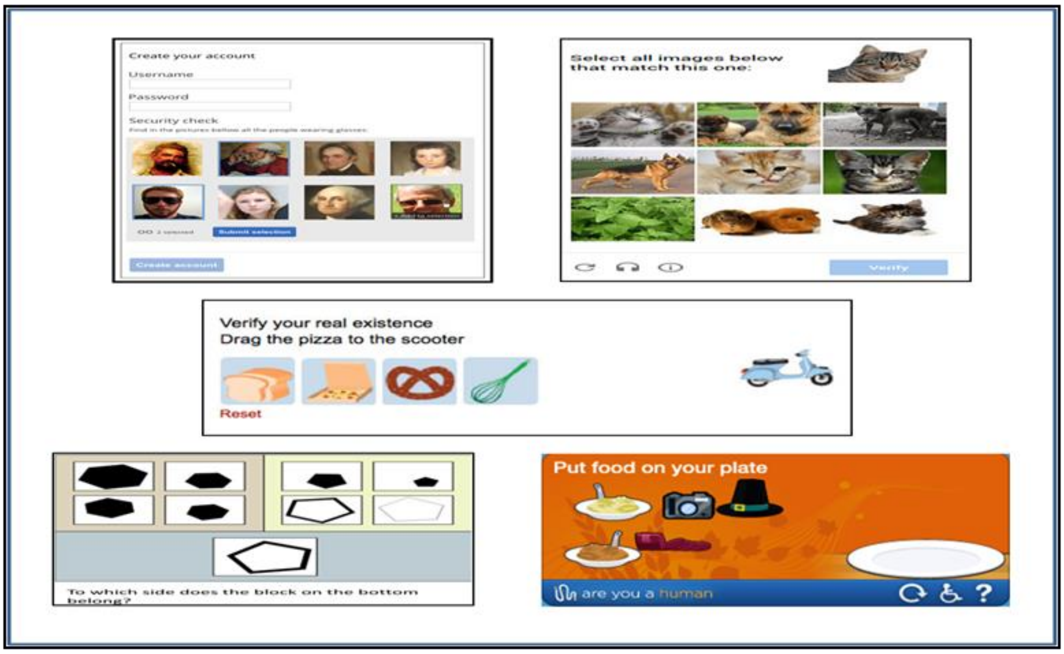
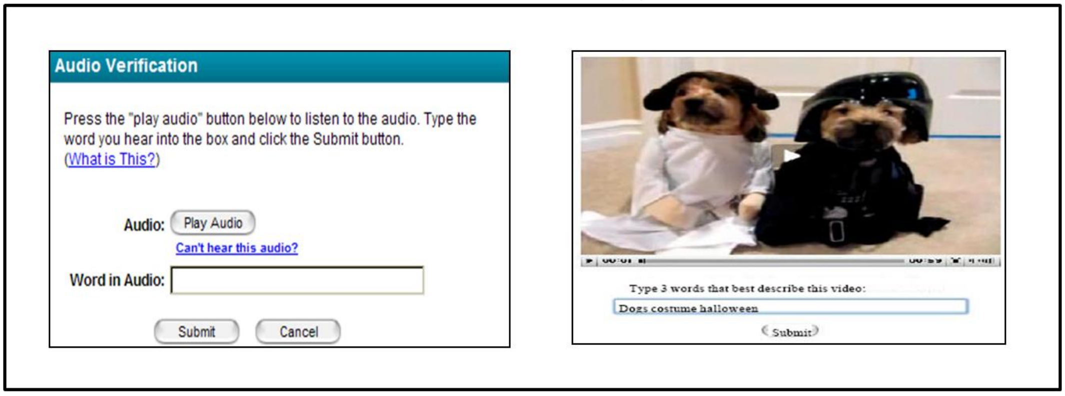

Create your account
Username
Password
Security check
Submit selection
Create account
Select all images below that match this one:
Verify
Verify your real existence
Drag the pizza to the scooter
Reset
To which side does the block on the bottom belong?
Put food on your plate
are you a human

Figure.3. Image based Captcha methods

In the sound based Captcha methods [6] the user must identify and type the word from the sound clipping. In order to improve the security the words and letters in the sound clip are distorted with background noise. This Captcha is mainly useful for the visually challenged people. In the video based Captcha [7] a video clipping is played to the user, and the user need to identify the words or characters in the video to get authentication. Figure.3. shows the audio and video Captcha images.



Audio Verification

Press the "play audio" button below to listen to the audio. Type the word you hear into the box and click the Submit button. (What is This?)

Audio: Play Audio

Can't hear this audio?

Word in Audio:

Type 3 words that best describe this video:

Dogs costume halloween

Figure.4. Audio and Video Captcha images

3. Captcha Applications

Captcha security methods have a variety of applications to keep the websites and web applications secure. It is incorporated almost in all types of login forms, account signup pages, online polls, and e-commerce checkout pages. The applications of Captcha is enormous which includes,

- Protecting email addresses from scammers
- Sustain website registrations
- Ensure fair online polling
- Protects against email worms
- Prevents dictionary attacks on passwords
- Prevents comment spamming on blogs

4. Captcha Design Issues

The two major issues in Captcha design are

- Security
- Usability

4.1 Security Issues

Any Captcha design should be,

- Easy for Generation, Implementation and Evaluation
- Easy for Humans to solve and Hard for bots

The text based Captcha methods are more user friendly. It is easy for all section of humans irrespective of age and education background. Hence the usability is very high. But it suffered by numerous automated bot attacks. In order to increase the security level, the Captcha design has been modified day by day. The Captcha characters are introduced with more twist, more distortion, overlapping of characters, background noise etc., which makes them robust to any kind of bot attacks. However it endures usability problems. Similarly the image based Captcha also cracked by various image matching algorithms and techniques. The usage of audio and video Captcha are very limited due to its generation issues. The hackers created various methods to break the Captcha images and to perform malicious activities in the websites. Automated bot attacks on Captcha become a challenge for the web security. The different types of Captcha attacks are,

- *OCR software attack:* The optical character recognition is one of the most common attacks on Captcha image. The process involves artificial intelligence, pattern recognition and computer vision. Bots acquire the Captcha images from the signup page by scanning process. The Captcha characters are identified by segmentation and recognition techniques and then submitted in the text box to gain access into the web service by automated OCR softwares [8].

- *Paid Human solvers or relay attack*: The bots gather Captcha images from Signup page and send immediately to the human solvers. The paid human solvers in a remote place solve the Captcha and send back to the bot. Now the bot is able to gain access into the website[9][10]

- *Laundry attack*: The Captcha attackers channel their bots automatically to send the Captcha to a malicious site and attract its visitors to solve the Captcha on behalf of them and make use of the answer for authentication [11].

- *Brute Force attack*: In this the attacker tries to gain access the web services by guessing every possible combination of Captcha characters that create the correct Captcha. This indicates that Captcha with short length of characters can be revealed and guessed easily.

- *Dictionary attack*: A dictionary attack is a method used to break the Captcha characters. It attempts to defeat the Captcha by systematically entering each word in a dictionary as Captcha in the text box and try to secure authentication. Dictionary attacks become successful when ordinary words are used as Captcha because they are easily found in an English dictionary [12].

- *Pixel Count attack*: In the Pixel count attack, the number of foreground pixels is counted in each segmented character and the characters in the segment are identified from the pre computed look up Table [13].

There are a large number online Captcha breaking services also, which provide free or paid service to break the Captcha images.

4.2 Usability Issues

Usability is another important issue in Captcha design. If the Captcha design is too complicate then the users will leave the website simply without utilizing the web service. Hence to attract the users the design of Captcha should be user friendly. The following important usability issues are needed to be focused in the design of Captcha [14].

- Distortion
    - How much the characters are distorted
    - How many confusing characters
    - How much alignment between characters
- Length
    - Length of Captcha characters
    - Character set – only characters / numerals / combination of both.
    - Random / fixed
- Presentation
    - Font size
    - Font type
    - Font color
- Background
    - Background noise
    - Background color
    - Clutters

The ultimate aim is to build a Captcha system as simple as possible so that the usability of Captcha should be increased, without compromising security. The Captcha should be very perception friendly. Perception is a human activity which connects the internal thought process between stimulus and response. Figure.4. shows some of the Captcha images which impart perception difficulty to humans. The Captcha design with less usability and simplicity give annoyance to the users which ultimately results to leave the website. These Captcha images are generated with more twist, added overlap, mystified background noise and complicated design.

A survey has been conducted with various sections of online uses to find the difficulty level, response time and success rate of various Captcha images and to identify the perception difficulty level. Their response on perception; execution difficulty level, execution time and success rate are noted as shown in Table.1.

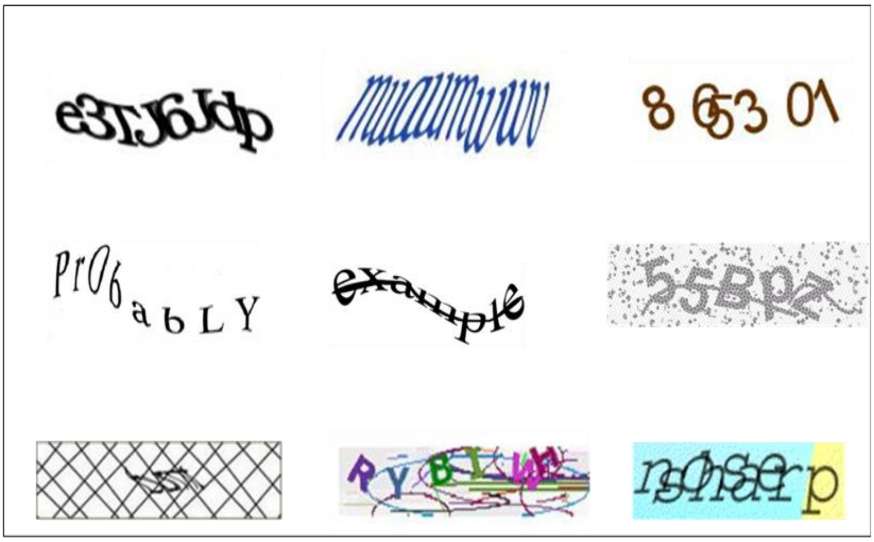
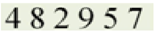
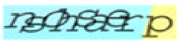


Figure.4. Poor perception Captcha images

Table.1 Response time analysis

Sl.No	Captcha	Type	Difficulty level	Ave.Exe.time (sec)	Success Rate (%)
1		Clear Perception	Very Low	5.3	100
2		Clear Perception	Very Low	6.3	100
3		Clear Perception	Low	6.8	100
4		Poor Perception	Low	7.2	100
5		Poor Perception	Medium	8.8	100
6		Poor Perception	Hard	14.7	65
7		Poor Perception	Hard	17.4	70
8		Poor Perception	Very Hard	28.9	40
9		Poor Perception	Very Hard	26.8	35

It is obvious to note that the users prefer perception friendly Captcha methods only because the difficulty level and execution time are low whereas the success rate is very high.

5. Conclusion

The Internet world needs more security from the automated malicious bots. It is learnt that more than 90 % of the websites uses text based Captcha only, as it is very simple for generation, execution and validation. Text based Captcha methods are user friendly when compared to other Captcha methods, but it endures security issues. With the aim of improving the security, the Captcha characters are twisted, overlapped and noise added in background to confuse the bots. But this tactics reduces usability and becomes a challenge for the human perception also. The other Captcha methods such as Image, audio and video based methods are also frequently suffered with different types of attacks. Hence more novel Captcha methods are needed with more security and user friendly.

References

[1] Luis von Ahn, Manuel Blum and Nicholas J. Hopper, 2003, 'CAPTCHA: Using Hard AI Problems for Security', in: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Poland.

[2] Zhaosheng Zhu, 2008, 'Botnet Research Survey', in: Annual IEEE International Computer Software and Applications Conference, IEEE.

[3] Ved Prakash Singh, 2014, 'Survey of Different Types of CAPTCHA', International Journal of Computer Science and Information Technologies, vol. 5, no.2.

[4] Elie Bursztein, 2014,' Easy Does It: More Usable CAPTCHAs', in: Conference on Human Factors in Computing systems, Toronto, Canada.

[5] Elson, 2007, 'Asirra: a Captcha that exploits interest aligned manual image categorization', in: Proceedings of the 2007 ACM, pp 366–374.

[6] Gao et al, 2010, 'An audio CAPTCHA to distinguish humans from computers', in: 3rd International Symposium on Electronic Commerce and Security, pp 265–269.

[7] Kluever, K.A., 2008, 'Evaluating the Usability and Security of a Video CAPTCHA', Rochester Institute of Technology, Rochester, New York, August.

[8] Prerna Sharma, Nidhi Tyagi & Deepali Singhal, 2013, 'Captchas: Vulnerability To Attacks', International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue.2.

[9] Marti Motoyama et al, 2010, 'Re: CAPTCHAs – Understanding CAPTCHA Solving Services in an Economic Context', in: Proceedings of the 19th USENIX conference on Security, Pages 28-28.

[10] Priyanka, Harleen Kaur & Dileep Kumar Kushwaha, 2013, 'Reviewing Effectiveness of CAPTCHA', International Journal of Computer Trends and Technology (IJCTT), volume 4, Issue 5.

[11] Elias Athanasopoulos, 2006, 'Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart', Lecture Notes in Computer Science, Springer, vol.4237.

[12] Chanathip Namprempre & Matthew Dailey, 2004, 'Mitigating Dictionary Attacks with Text-Graphics Character CAPTCHAs', in: TENCON 2004 Conference Proceedings, IEEE.

[13] Jeff Yan, Ahmad Salah & El Ahmad, 2009, 'CAPTCHA Security-A Case Study', IEEE Security & Privacy, volume:7, Issue: 4.

[14] Jeff Yan, 'Usability of CAPTCHAs or usability issues in CAPTCHA design', in: Proceedings of the 4th Symposium on Usable Privacy and Security, New York.