ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

A DETAILED EXPLANATION OF THE CAPTCHA TO IMPROVE SECURITY.

Vignesh Jeevan.
Computer Science and Engineering, Sathyabama University, Chennai, India.

Manuscript Info

Manuscript History:

Received: 18 March 2016
Final Accepted: 10 April 2016
Published Online: May 2016

Key words:
Numerical captcha, Image captcha, Video captcha.

****Corresponding Author***

Vignesh Jeevan.

Abstract

This paper proposes the latest attacks which are been done in the internet. It explains how these various attacks can be stopped by using various techniques of captcha. There are various types of captcha available nowadays. This paper explains how we can improve the internet security by using the advance captcha. There are two types of captcha which we have seen they are: Numerical captcha and image captcha. In this paper we explain about the advance version of captcha like the motion graphical captcha, pictorial captcha. These captcha can be used for various purposes. It can be used for email verification, bank details verification and even for other payment options. These captcha increases the security from getting the websites hacked.

Introduction:-

In this paper we are going to discuss about the various captcha. There are two types of captcha which are used nowadays. These captcha are good but not that good. These captcha can be easily hacked by the hacker. To improve the security we are going to introduce two new captcha which will make the hacker to hack the captcha. The captcha should be not predefined or the captcha should not be given by the server. The captcha should be decided and solved only by the user.

The main purpose of using the captcha is to provide the security to the email, banking websites or other payment websites. As these websites may contain authentic information in which the other users should not be able to access those information. If the hacker is able to crack the captcha, the hacker can access the most authentic information of the user. The captcha should prevent the robots or the hacker from providing entry to the emails. The captcha should be limited to the minimum number of times to solve.

The captcha is mostly used to check whether the person who is trying to access is not a robot or a hacker. The captcha should be made difficult because if the hacker is able to crack the captcha, then all the authentic information would be available to the hacker. The captcha can be made in such a way that the captcha can be solved minimum number of times. By limiting the uses the captcha will be protected from the hackers and the robots.

Existing System:-

The current system has two types of captcha. i.e. Numerical captcha and image captcha. Numerical captcha is a type where the user is given a set of numbers. The user has to type the given numbers. If the numbers given are correctly typed by the user then the user is allowed to proceed. The captcha is mainly used to prevent the phishing attacks.

The phishing is mainly done using the mail message, where the attacker sends the email to the users. These messages take the sensitive information of the users. The information could be the email password or the credit card number of the user. Sometimes the attacker creates the webpage where the user has to survey for the required website. As the user enters the information in the survey form the attacker gets the sensitive information of the user.

The attackers create a similar website or mimic the legal website which makes the user difficult to identify the fake website. The phishing has grown in greater diversity where the sensitive information is send all through the emails.

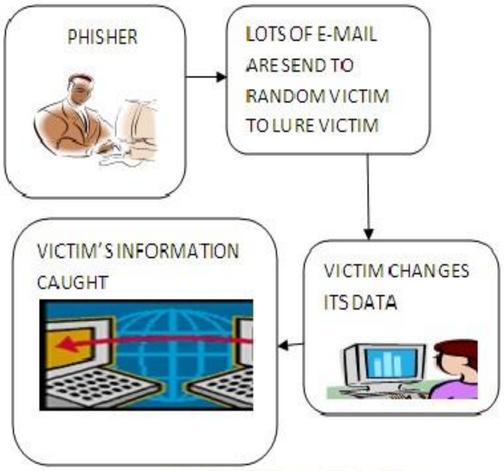

PHISHER
LOTS OF E-MAIL ARE SEND TO RANDOM VICTIM TO LURE VICTIM
VICTIM CHANGES ITS DATA
VICTIM'S INFORMATION CAUGHT

Fig: Phishing of Emails

The above figure show how the email are been attacked. These attacks can be reduced by using the captcha. The email can be easily hacked by the hackers and they can also change the data.
Phishing attack is a stage based approach.

- The attacker gets the users email address by various sources.
- The attacker sends the link of his fake website to the users email address.
- As soon as the user opens the link the sensitive content gets into the hand of the attacker.

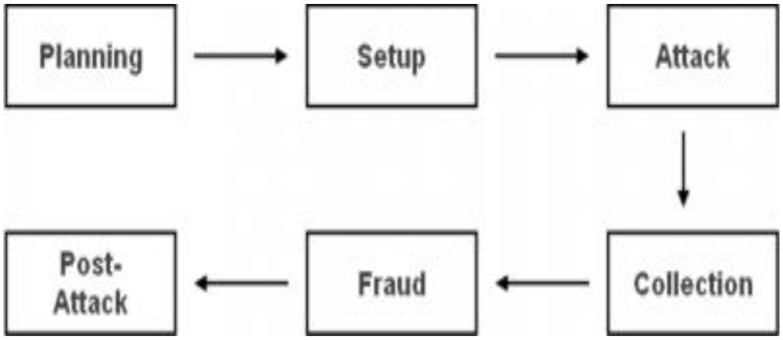


Fig: Stages of the phishing attacks.

The above diagram shows the stages of the attacks. The approach starts with the planning where the attacker plans to attack on the user. The attacker tries to attack the email by sending malicious mail to the user. After the successful attack the attacker collects the useful information from the user system. According to the plan the attacker attempts for the post attack.

The stages could differ accordingly to the attacker. Sometimes the user gets useful (sensitive) information and then attacks using those information. The attacker always ties to get the information from the user. As the attacker gets the information the attacker may perform hacking only when the user goes offline.

Modules:-

Numerical Captcha

The numerical captcha is mostly used in most of the websites. This captcha is mostly used to validate the user. The numerical captcha consists of the numbers. The user has to type the given numbers in the give text box. The entered captcha is validated in the server, if the captcha is correct the user is allowed to proceed to the next page.

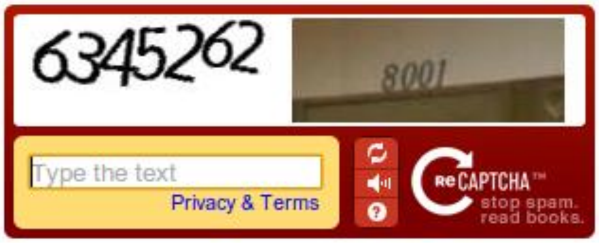


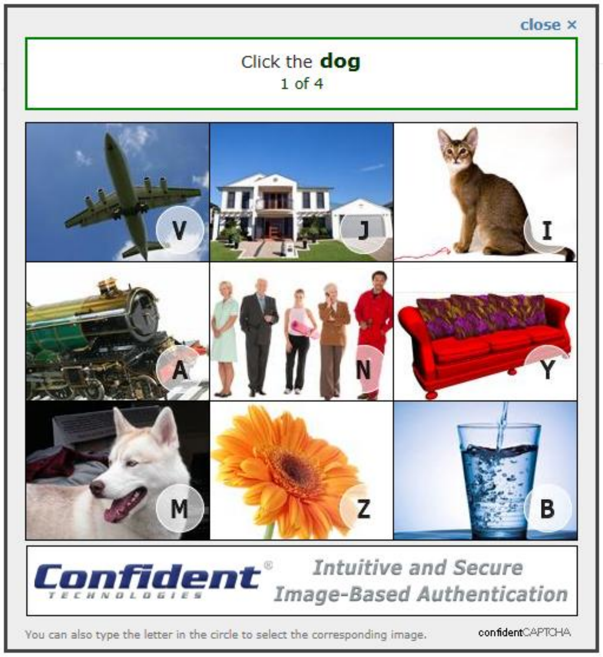
Fig: A view of Numerical Captcha

The above figure shows the numerical captcha. This captcha has the numbers given. The user has to type the given number in the text box.

The numerical captcha does not provide much security to the website. As these captcha are easily hacked by the hacker or the robots. The numerical captcha does not protect the users from malicious attacks. These captcha needs to be improved. The improvement can be in changing the interface of the captcha. The captcha can include some pictorial images, where those images are difficult to hack by the robots.

Image Captcha:-

The other type of captcha is the image captcha. This type of captcha is similar to numerical captcha. The image captcha consists of image. The captcha contains more than five images. The user has to select one of the images. The image has to be selected by the question given in the captcha. If the user selects the correct image the user is allowed to move to the next page.


Click the **dog**
1 of 4

You can also type the letter in the circle to select the corresponding image.

Fig: A view of Image Captcha.

The above figure is the image captcha. The above captcha asks the user to select the image with the dog. If the user selects all the images with dogs the captcha is solve. If the user even misses a single picture of dog the captcha remains unsolved.

The image captcha has more security than the numerical captcha. The image captcha cannot be easily solved by the hacker or robot. Although there are some chances that the image captcha can be hacked by the robots. To improve the security we use other type of captcha i.e. Motion Graphical Captcha. This captcha is different than the other two captcha. This captcha allows the user to move the object in the given window.

Motion Graphical Captcha:-

This captcha is the most secure captcha. This captcha improves the security of the webpages. This captcha can be used in any of the websites like e-mail, online payment websites, online ticket reservation websites.

This captcha has an object which allows the user to move that object. The server will give the combinations to solve the captcha. These combinations will change every time the user visits the website. The user has to drag that object according to the combinations. If the combinations are correct the user can move to the next page.

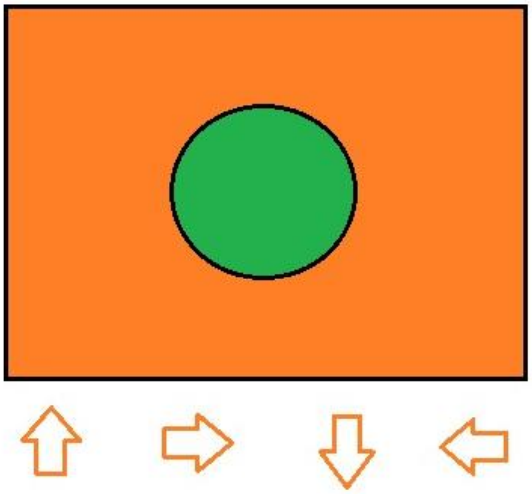


Fig: Motion Graphical Captcha.

The above figure shows the object where the user has to move the object with respect to the combinations given below.

References:-

1. The Antiphishing Working Group (2010) Home Page, http://www.anti- phishing.org.
2. Ollman, G. (2011) The Phishing Guide – Understanding and Preventing, White Paper, Next Generation Security Software Ltd.
3. The Antiphishing Working Group (2011) Phishing Activity Trends Report, http://www.anti-phishing.org.
4. Jyoti Chhikara, Ritu Dahiya, Neha Garg, Monika Rani,” Phishing & Anti-Phishing Techniques: Case Study”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, ISSN: 2277 128X ,Page 458-465 , May 2013.
5. C. Emilin Shyni and S. Swamynathan,”Protecting the Online User Information Against Phishing Attacks Using Dynamic Encryption Techniques”, Journal Of Computer Science,9(4):526-533,ISSN 1549-3636, 2013.