

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Phishing Detection Using Visual Cryptography

Prasad Mahajan¹, Snehal Mule², Shalaka Ekawade³, Neha Chandrapatle⁴, U.C Patkar⁵

BE. Student, Department of Computer Engineering, BV Engineering College, .Pune, Maharashtra, India¹

BE. Student, Department of Computer Engineering, BV Engineering College, .Pune, Maharashtra, India²

BE. Student, Department of Computer Engineering, BV Engineering College, .Pune, Maharashtra, India³

BE. Student, Department of Computer Engineering, BV Engineering College, .Pune, Maharashtra, India⁴

HOD, Department of Computer Engineering, BV Engineering College, Pune, Maharashtra, India⁵

ABSTRACT: Now-a-days online attacks have increased to a great extent and the most popular attack among them is phishing. Phishing can be basically defined as one kind of attack in which various attackers acquire the confidential and sensitive information of the victims. The Phishing is an attempt by an individual or a group to thief personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. In phishing attack phishers attempt to fraudulently acquire sensitive information like users id, password, contact details, credit card information etc. by masquerading as a trustworthy person or business in an electronic communications. Thus, security in such cases should be very high to avoid the online attacks. So it is very much important for users to identify the fake website and avoid falling prey to it. Here an image based authentication using Visual Cryptography (vc) is used .The main aim of visual cryptography is to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers.

KEYWORDS: Phishing, Visual Cryptography, Image , Captcha, Share Generation.

I. INTRODUCTION

Today, most applications are not that secure. Sometimes, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered as secure or not. Phishing scams are also becoming a problem for online banking , financial web portal etc. Here the big question is how to handle applications that require a high level of security. Here an image based authentication using Visual Cryptography (vc) is used. The use of visual cryptography is used to preserve the privacy of image captcha by dividing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed. Once the original image captcha is revealed to the user it can be used as the password. The utilization of visual cryptography is investigated to safeguard the privacy of a picture captcha by breaking down the image captcha into two shares that are put away in separate database servers such that the first picture captcha can be uncovered just when both are all the while accessible; the individual sheet pictures do not uncover the character of the first picture captcha. When the original picture captcha is uncovered to the client it can be utilized as the secret word. Utilizing this site cross checks its character and proves that it is a certified site before the end clients.

II. RELATED WORK

Online trasactions in 21st century becoming very common in daily use, various different techniques are employed by an single people or group of people to perform fradulant activities, i.e. phishing web pages which is involves use of

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

creating fake web sites or pages which are similar to real web pages or sites and is presented to user. Sometimes these web pages are as it is similar to the original web pages and these web pages is look exactly like real web page. On the basis of these fake web pages victims of phishing web pages expose their bank account, credit card number, personal information or important information to the phishing web page owners. Middle man attacks are common where data is obtains while data traverse over network thus data security and phishing is an important area where work needs to be done.

Emails are most common techniques for phishing because of simplicity and easy use with wide reach. Attacker can deliver specially crafted emails to millions of legitimate email addresses very quickly and can fool the recipients utilising well known flaws in the SMTP.

III. TEXT IMPLEMENTATION

There are two phases in implementation, they as follows:

1. Registration Phase
2. Login Phase

1. Registration Phase

In the registration phase, a key string i.e. password is asked from the user at the time of registration for the secure website .this string concatenated with randomly generated string in the server and an Image CAPTCHA is generated. The image CAPTCHA is divided into two shares. In which one share is kept for user side and another share is kept in the server. The user's share and the original image CAPTCHA is sent to the user for later verification during login phase. This image CAPTCHA is also stored in the database of any confidential website as confidential data. After registration, the user can change the key string when it is needed.

2. Login Phase

When user login in by entering his confidential information for using his account then first user is asked to enter his username. In the Login phase first the user is prompted for the username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website, for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.

Internal working divided into three parts:-

1. Generation of image CAPTCHA
2. Encryption (Creating Shares)
3. Decryption (Human Visual System)

1. Generation of image CAPTCHA

CAPTCHA image is mainly used for giffering human users and computer programs from each other.CAPTCHA text consider of characters and numbers which text is composed of five charactyers and each character has its bending and asize value.

There are four steps for generating image CAPTCHA

Step 1: Start

Step 2: Generate n letters random string from the string

“ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789”

Step 3: Use the Random() function string of length 'n' and put it into the session

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Step 4: Create transparent CAPTCHA image with w by h image size and add CAPTCHA text over it.

2. Encryption:

In the Encryption process an image CAPTCHA has been considered in our design where each pixel is either 0 i.e. Black or 1 i.e. White is original binary image.

Pseudo code for Encryption process is given as below:

```

For I = 1 to Size of the image
  If ( pixel == 1 )
    If ( random == 1 )
      Share 0 = [ 1  0 ]
      Share 1 = [ 1  0 ]
    Else
      Share 0 = [ 0  1 ]
      Share 1 = [ 0  1 ]
  Else
    If ( random == 1 )
      Share 0 = [ 1  0 ]
      Share 1 = [ 0  1 ]
    Else
      Share 0 = [ 0  1 ]
      Share 1 = [ 1  0 ]
  End
End For Loop
  
```

3. Decryption :

In the decryption process use reverse process of encryption. In this process perform bitwise logical AND and OR operation performed on two obtained share images from previous stage to get back the retrieved image. The obtained image is identical to original image.

There are two steps are involve ed:-

step 1: overlaid version of encrypted image is regerated by AND'ing each pixel position wise.

Step 2: Regerating the original encrypted image from the overlaid version by OR'ing these pixel value of overlaid version .

IV. EXPERIMENTAL RESULTS

Figures shows the results of Antiphishing framework from an image and by using VC (2,2) algorithm. Fig (a) shows the Login framework. Fig(b) is the Registration framework. Fig (c) shows the downloading of image captcha.

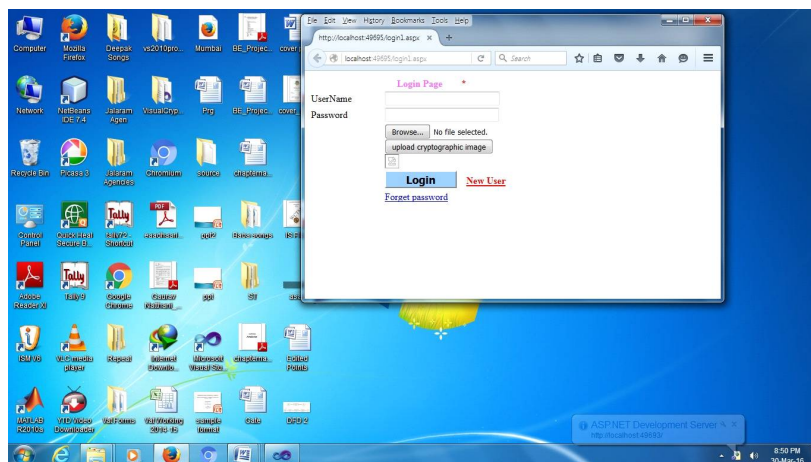


Fig. a is showing the Login framework.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Login phase is the phase where the user needs to enter the username and upload the cryptographic image and then login. If the login is successful then the user can enter the password. The login phase plays an important role in this framework.

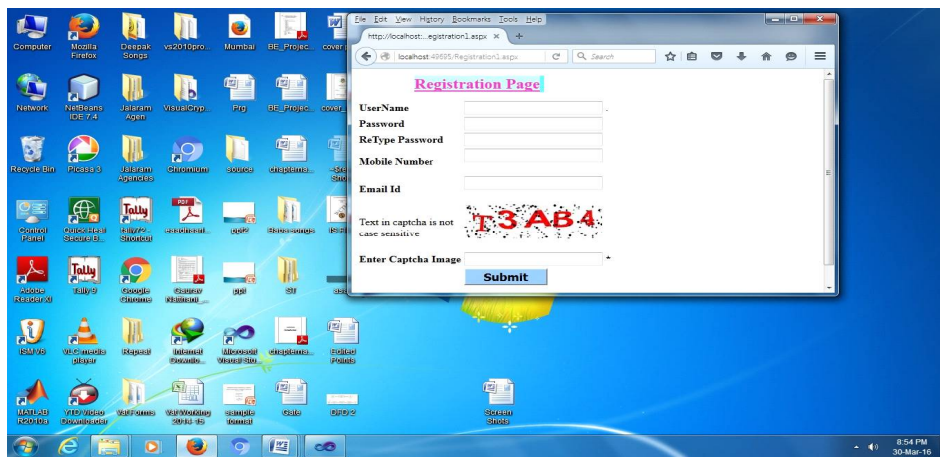


Fig. b is showing is the Registration framework.

In Registration phase user needs to register the details so that user details are not misused by any other person. It consists of username, password, re-type password, mobile number, email id and most important is to enter the captcha.

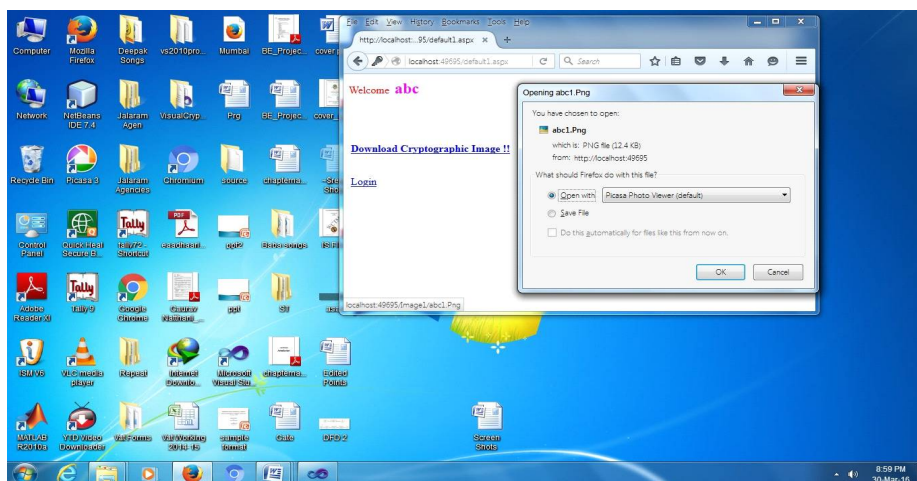


Fig. c is showing the downloading of image captcha.

After registration phase user needs to download the cryptographic image. The share of cryptographic image is divided into two shares. One share is kept at the user side and other share is kept at server side. At the specified path the image is saved.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

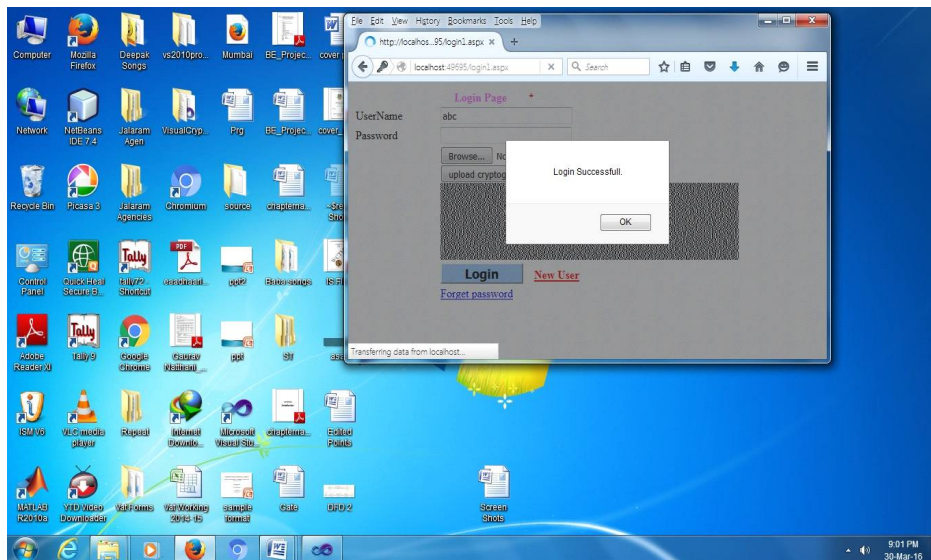


Fig. d is representing successful login by using correct share and password.

When user upload the cryptographic image, image should get matched with the share which was been shared at the registration phase. If the image uploaded is same then the login is successful or otherwise it is not.

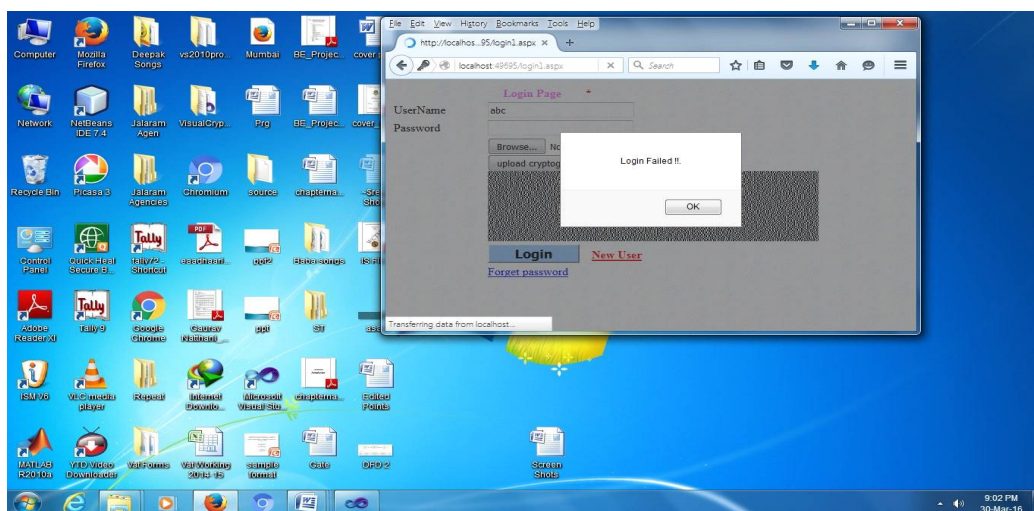


Fig. e is showing unsuccessful login because of invalid share.

When user upload the cryptographic image, image should get matched with the share which was been shared at the time of registration phase. If the share is valid then login is successful. If the share is invalid then the login is failed.

V. CONCLUSION

Now-a-days internet is used on a large scale so the phishing attacks are becoming very common. The phishing attacks can globally acquire the user's confidential information like username, credit card number, and password, etc. And this

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

data may be stored on to the database and may be used for the illegal purposes. Phishing is basically the attack mainly done to gain the access to confidential information of the victims. By using the proposed method of —Anti-phishing Structure Based on Visual Cryptography and RSA Algorithm phishing websites can be identified. Thus with help of the techniques used in the paper we can successfully helped the users to identify the fake and genuine website so that he doesn't fall prey to the phishing attacks. Thus the security purpose gets served here.

REFERENCES

1. W.-G. Tzeng and C.-M. Hu, "Anewapproach for visual cryptography," *Designs, Codes, Cryptog.* vol. 27, no. 3, pp. 207–227, 2002.
2. C. N. Yang, "New visual secret sharing schemes using probabilistic method", *Pattern Recognit. Lett.*, vol. 25, pp. 481-494, Mar 2004.
3. C.-N. Yang and C.-S. Laih, "Some new types of visual secret sharing schemes," in *Proc. Nat. Computer Symp*, vol. 3, pp.260–268. 1999.
4. C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques", *Pattern Recognit. Lett.* vol. 24, pp. 349358, Jan. 2003.
5. Moy, G., Jones, N., Harkless, C., Potter, R., "Distortion estimation technique in solving visual CAPTCHAs", *Proc. ofthe 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2004*, vol.2, pp.23-28,2004.