www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 14009-14014

Detecting Phishing Websites Based On Improved Visual Cryptography

Reshma Ramdas T

M. tech student, Department of Computer Science and Engineering
Al-Azhar College of Engineering and Technology, Perumpallichira, Idukki, Kerala, India
reshma440@gmail.com

Abstract: ***Most of the time people using internet for online transactions from one place to another place because of its cost effectiveness and ease of use. So it is necessary to ensure the security of such transaction but unfortunately an attacker can attack on system online or offline. Among a various kind of internet attacks, phishing is identified as a major security threat and all the prevention mechanisms failing in front of that, so prevention mechanism should be very strong. Phishing is defined as an identity theft attempt in order to obtain confidential and private information of individuals or companies for monetary or other gains. If these threats are not addressed thoroughly, people can't trust online transactions that involve due authentication through credentials. A visual cryptography based technique will automatically preserve the privacy of captcha during registration. It is done by dividing the original image captcha having the password into two shares which are to be stored in different databases. The decryption is possible only when adversaries can provide both shares at a time. The individual shares can't reveal the original captcha. In the proposed methodology discusses the security to the user share by implementing AES PKC5 Padding encryption algorithm which guarantees the confidentiality of the user share from attacks.***

Keywords: AES PKCS 5, DNS,URL, VCS**.**

Introduction

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. The most popular phishing scams are carried out using phishing web pages. Phishing web pages are forged to mimic certain legitimate companies' web pages. Phishing websites usually trick users into leaking their sensitive information and private data by counterfeiting trustworthy web identities. Unwary users may easily be deceived by such scams.

Victims of phishing web pages may expose their bank accounts, passwords, credit card numbers, or other important information to malicious people. Thus the security in these cases be very high and should not be easily tractable with implementation easiness**.**

Therefore, an efficient online transact fraud detection system called anti-phishing is badly needed by merchants to protect the legitimate customer, to lower the maintenance costs and to increase public confidence and trust in online transactions.

1. Motivation and Related Works

Phishing attack has become common in various organization including both private and government firms. Hence Many types of anti-phishing techniques have been introduced to resolve such phishing problem, and such anti-phishing techniques are applied at both client side and server side.

2.1 **Identity Based Anti-Phishing Techniques**: In this technique mutual identification is done where the user and visiting site checks each other identity while handshake. It is an anti-phishing technique which integrates partial credentials sharing and client filtering technique to prevent phishes from easily masquerading the online websites. As mutual authentication is followed, there would be no need for users to re-enter their credentials. But here, if an attacker gain access to the client computer and disable the browser plug-in then method will be compromise against phishing detection.

2.2. **Automated Challenge Response Method (ARM**) is one such authentication mechanisms where challenge generation module in server requests for response from Challenge-Response interface in client. Then Challenge-Response module calls get response application installed in client machine. Once this is done, user credentials are demanded from client and it is validated by server and thus transaction is made secure.

This ensures two way authentications and also prevents man-in-middle attacks as response is obtained from executable which is called by browser and third man cannot interrupt at any cost.

2.3. **Blacklist based technique** is a DNS based anti-phishing approach commonly used by browsers. But the Shortcoming of this technique is it has low false alarm probability, but it cannot detect the websites that are not in blacklists. Life cycle of phishing websites is too short for establishment of blacklists which makes this technique inaccurate.

2.4. **Heuristic-based anti-phishing technique** is a technique where a webpage is checked to find out whether the page has any of the phishing heuristics characters like host name, checking URL for common spoofing techniques [3] and checking against previously seen images. This method does not yield accurate results as even the attackers are aware of such techniques and they use some strategies so that they are not detected. And then find out whether the page has any of the phishing heuristics characters like host name, checking URL for common spoofing techniques [3] and checking against previously seen images. This method does not yield accurate results as even the attackers are aware of such techniques and they use some strategies so that they are not detected.

2.5. **Similarity assessment based technique** is time swallowing, it need too more time to deliberate a couple of pages, so using the method to diagnose fraud websites on the client terminal is not fitting. And there is low correctness rate for this method depends on many factors such as the word, photographs and equivalence measurement technique.

2. Existing System

Different from the conventional anti-phishing methods later on Divya James and Mintu Philips [7] proposed anti-phishing framework using visual cryptography where they referred work done by M. Naor and A. Shamir on visual cryptography and they used this technique to build anti-phishing framework.

Registration Phase

In the registration phase, user enters a key, server enters a key and them captcha image is presented. The image is divided into two shares in such a way that the shares when stacked together should restore the original captcha.

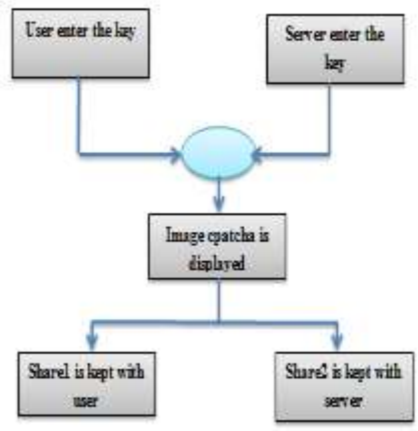

Fig. 3.1 Mechanism in registration phase

In the registration phase, a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. According to the key given by the user this string is concatenated with randomly generated string in the server and an image captcha is generated. So the new image captcha is processed behind. By this dynamic generation the theft by camera can be easily avoided. Then “Blowfish Algorithm” is applied to divide the original image captcha into many blocks and rearranged. Then “Splitting and Rotating Algorithm” is applied to rotate the rearranged blocks.

The image captcha is divided into two shares by (2,2) visual cryptography scheme such that the image captcha is divided according to black and white pixels. Then one of the share is kept with the user and the other 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. The image captcha is also stored in the actual database of any confidential website as confidential data. Because the image captcha is used as the password later. After the registration, the user can change the key string dynamically when it is needed.

Login Phase

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to upload 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.

By 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.

When user attempts to log in into site , in order to increase more security the image captcha is encrypted using many algorithms. This encryption Phase contains many algorithms like Blowfish, Splitting and Rotating algorithm and (2,2) Visual Cryptography Scheme. First the “Blowfish Algorithm” is applied to the original image captcha then the image captcha is divided into many blocks and rearranged.

After the image captcha blocks are rearranged, the “Splitting and Rotating Algorithm” is applied to the image captcha, then the rearranged blocks are rotated. Then the rearranged and rotated blocks are combined. Then (2,2) VCS scheme is applied to the combined blocks. This scheme is used to divide the encrypted image captcha into two shares based on white and black pixels. When the two sub pixels are identical blocks it consider as a white pixel. Likewise when the two sub pixels are different the original pixel is consider as black pixel. This VCS scheme adds more complication to the image captcha. At last one of the share is kept with user and another part of the share is kept with server. When two shares are stacked together and the reverse process of encryption taken place the original image captcha is revealed. From this the user can check whether the website is original or fake .At the same time the server can verify that whether the user is human being or robot.

In the login phase actual authentication takes place. The authentication process is built in such a way that it can detect any kind of phishing attack.

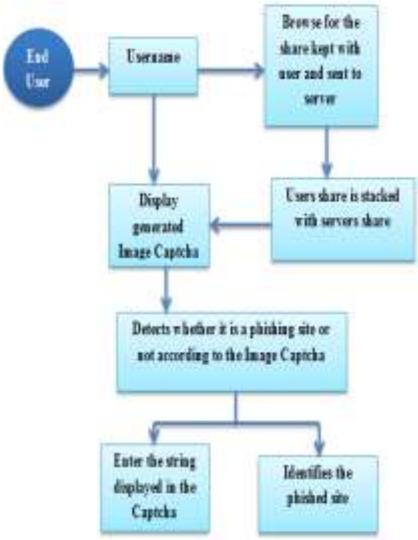
End User
Username
Browse for the share kept with user and sent to server
Users share is stacked with servers share
Display generated Image Captcha
Detects whether it is a phishing site or not according to the Image Captcha
Enter the string displayed in the Captcha
Identifies the phished site

Fig.3.2 Login Phase mechanisms for anti-phishing

As shown in fig, the end user given credentials and then chooses the share of the captcha given to him at the time of registration. Then the server sends its original captcha can find whether the user is really genuine user or a phishing attack is carried out. The login mechanism can identify phishing activity and prevent it efficient with 100% true positives.

4. Proposed System

The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image.

In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system.

The different VCS access structure schemes.

1. (2, 2)- Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.

2. (n, n) -Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed.

3. (k, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Figure.3.1 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

Implementation

For phishing detection and prevention, here proposing a new methodology based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites. The more advanced AES PKCS5 Padding image encryption is used here to encrypt the image share with a 16bit user provided key which provide more security towards theft of the user share. The encryption is done at the client side and server side same time. A one time password is sent to the client securely thereby provide multilevel security against phishing. It offers lower computational cost since the secret message is recognized only by human eyes and no need to cryptographically compute it.

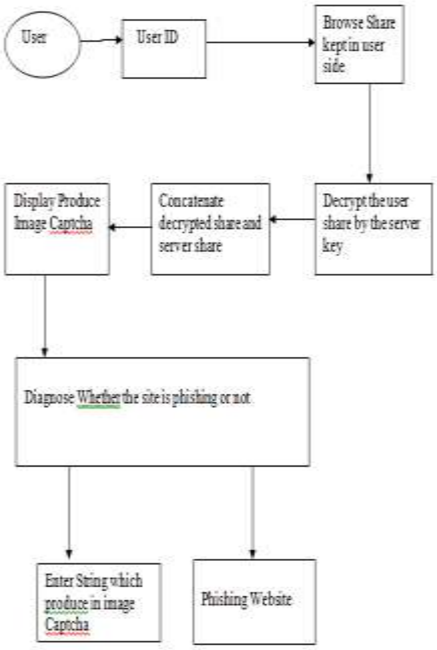
User
User ID
Browse Share kept in user side
Decrypt the user share by the server key
Concatenate decrypted share and server share
Display Produce Image Captcha
Diagnose Whether the site is phishing or not
Enter String which produce in image Captcha
Phishing Website

Fig.4.1 Architecture of the proposed work

Registration phase

In the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server.

The user share is encrypted by the client by a 16bit key and then allowed to download. The encrypted user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed.

Registration process is depicted in Figure.

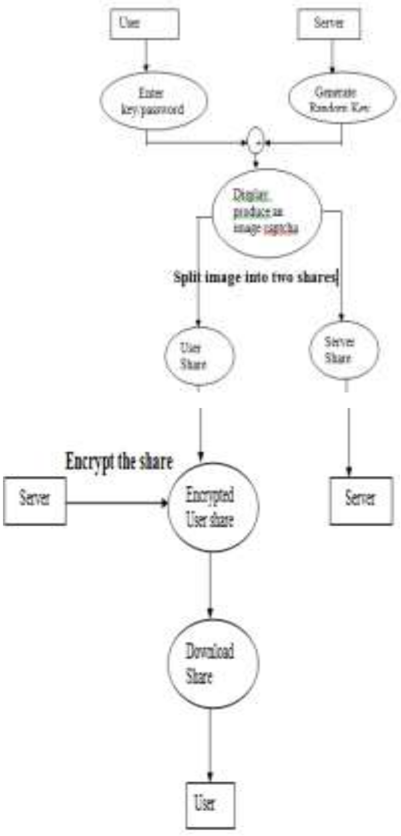

Fig 4.2 Registration Process

Login phase

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 firstly the server does decryption of the user share and 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.

Figure can be used to illustrate the login phase

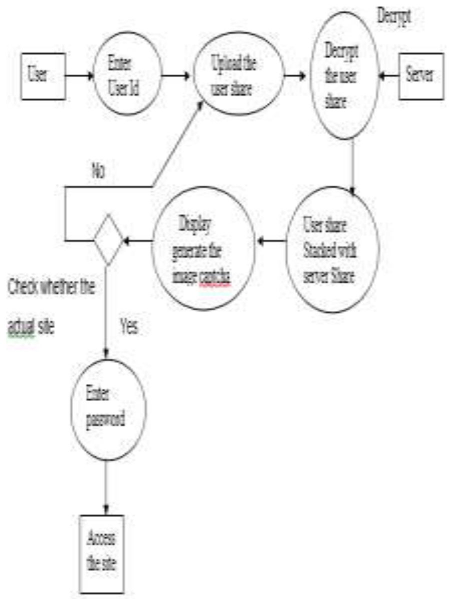

Fig 4.3 Login Process

5. CONCLUSION

This proposed methodology " Detecting phishing websites based on visual cryptography" preserves confidential information of users using three layers of security. First layer verifies whether website is secure one or not. In second layer check validity of image captcha .Only human user is capable of reading image Captcha. In third layer of security ensure the prevention against attacks from unauthorized user in user account. To ensure more safeguard from sophisticated attackers who try to acquire the user share the encrypted user share is provided to the user for future login hence there is no complexity in the client side. All the encryption and decryption is carried out in the server side.

.

References

[1] Mrs.A.Angel Freda, M.Sindhuja, K.Sujitha, IJREAT, Image Captchabased Authentication using visual cryptography vol.1, pp.2320-8791, April-May, 2013.

[2] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Moverâ Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, vol.3, pp.301-311,

October/December 2006.

[3] JungMin Kang, DoHoon Lee,IEEE, “Advanced White List Approach for Preventing Access to Phishing Sites””, pp.491-496, 2007

[4] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu,IEEE Internet Computing "An Antiphishing Strategy Based on Visual Similarity Assessment", vol.10, p 58-65, March/April 2006..

[5] Haijun Zhang,Gang Liu, and TommyW. S. Chow, IEEETrans. “Neural Netw, Textualand Visual Content-Based Anti-Phishing: A Bayesian Approach””, IEEE Trans. NeuralNetw., vol.22, no. 10, pp.15321546, Oct.2011.

[6] Divya James1 and Mintu Phillip2, ”A novel anti phishing framework based on visual cryptography”, vol.3, no...1. pp.1264-3459, January.

[7] Kundankumar Rameshwar Saraf1, Vishal Prakash Jagtap2, Amit Kumar Mishra3 “Text and Image Encryption Decryption Using Advanced Encryption Standard”, ISSN 2278-6856, Volume 3, Issue 3, May – June 2014

Author Profile

Reshma Ramdas T received the B.Tech degrees in Information Technology from MG University at Caarmel Engineering College in 2013. And now she is pursuing her M.Tech degree in Computer Science and Engineering under MG University, Kerala in Al-Azhar College of Engineering and Technology