ISSN 2395-1621

An Anti phishing framework using Visual Cryptography

[#1]Bhupali Bhoite, [#2]Varsha Rathod, [#3]Hina Shaikh, [#4]Shivanjali Bhapkar,
[#5]Mrs. Prof. M. N. Navale

[1]bhupalibhoite59@gmail.com
[2]rathodvarsha01@gmail.com
[3]shaikhhina91@gmail.com
[4]Shivu28_1994@yahoo.com

[#12345]Department of Computer Engineering,NBN Sinhgad School of Engineering, Pune-411041

ABSTRACT

In todays era, information security is very important in which data is secure from unauthenticated user. Unsuspected victims can attack the information for financial gain, individual gain and also for other illegal activities. Phishing is one of them in which, unauthenticated users tries to thieve the information which is personal confidential. To avoid such illegal activities we have projected a new paper named as "An Anti-Phishing Framework Using Visual Cryptography". In this, image is generated which after exploit, decomposes into two shares. One share is kept with user and other with bank server. And when it requires that is at the time of login at site, these two shares are combined together to form original image. The image form by combining two shares will state that current site is not a phishing site and also identify that user is authenticated one. So data can be secured from unsuspected user.

ARTICLE INFO

Article History

Received :24th May 2016

Received in revised form :

26th May 2016

Accepted : 28th May 2016

Published online :

30th May 2016

***Keywords*—** Information security, Steganography, Visual Cryptography, Online shopping.

I. INTRODUCTION

Nowadays online booking system, bank transactions, etc are very common. So while performing above mentioned activities, various attacks can hazard the information. Phishing attack is one of them in which illegal activities are performed using different social engineering techniques[1][3]. Attackers try to acquire crucial information such as password, credit card details and confidential data. Phishing can be defined as "The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online". To avoid such scenario there are two problems which we need to overcome. First one is to identify whether the site is phishing site or not and second problem is to identify that whether the user is authorised or not. So here we are introducing new technique which can be used as secure method against phishing named as" An Anti-Phishing Framework Using Visual Cryptography". In this technique website verifies its own identity and prove that it is a genuine website and also checks the users identity to avoid phishing. The frame work supports complete web application security. The proposed system has three phases first phase deals with user registration [1][2]. While making registration one image is selected by user from application site then it is converted into two share images[2]. In second phase user get share one of image which is encrypted at the time of exploitation of original image. To secure the share one at user side, user assigns a private key to that image which is necessary at the time of transaction. In third phase if user wants to do any transaction then it is a need to upload share one with private key set by user to share one , while at the other side server automatically uploads share two of original image[2][4].

II. LITERATURE SURVEY

Phishing web pages are illegally copied web pages that are created by malicious people to copy Web pages of real web sites. Mostly such kinds of web pages have high visual similarities to scam their victims. Some of such kinds of web pages look exactly like the real ones. Victims of phishing web pages may expose their bank account, password, credit card number, or other important

information to the phishing web page owners can be exposed by victims of phishing. It includes methods such as tricking customers through emails and spam messages, installation of key loggers, man in the middle attacks and screen captures.

The user-based mechanisms is proposed by researchers to authenticate the server. Automated Challenge Response Method[6] is one of the such authentication mechanisms which ,includes challenge generation module from server which in turn interacts with Challenge-Response interface in client and requests for response from the user.

Also there are DNS-based anti-phishing approach[7] technique which includes heuristic detection, blacklists the page similarity assessment. But they too have some shortcomings.

Heuristic-based anti-phishing technique is used to check whether a webpage has some phishing heuristic characteristics. For example, some heuristics characteristics used by the SpoofGuard [8] toolbar include checking the URL for common spoofing techniques, host name, and checking against images seen previously. The accuracy is not enough, If you only use the Heuristic-based technique.

Similarity assessment based technique is a time-consuming. It needs too long time to calculate a pair of pages, so by using the method to detect phishing websites on the client terminal is not suitable. And also there is low accuracy rate for this method which depends on many factors, such as images, the text and similarity measurement technique. However, this technique (in particular, image similarity identification technique) is not perfect enough yet.

III. USER REGISTRATION PHASE

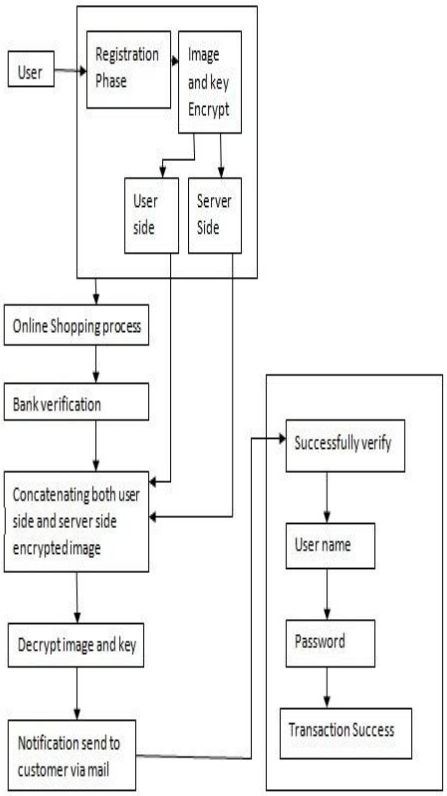
To do any online transaction one need to register to any bank which provides online banking. In this phase user registration is done with the help of Visual Cryptography Algorithm system. While registration of user with visual cryptography user choose the random image from his system itself[4]. The selected image should be remember by the user which is needed in future. After the selection of the image Visual Cryptography algorithm is applied on that image. Output of this phase will give two shares. Out of which first share goes under the process of phase two. And second share will recorded to server side with user id and original image.

IV. APPLY THE ENCRYPTION ALGORITHM

Now user completed the phase one. We need to give share one to user with secure approach. For that we assign the private key to the encrypted image. And store the private key to server side. When user goes for any transaction need to upload the share one and to authenticate himself, he need to give that private key.By this phase server can be easily identified.

V. DETECTION OF PHISHING SITE

When user goes for a transaction, user need to upload the share one[1][2][4]. After uploading, server will request for private key. User need to provide private key assigned during registration (in phase two). Now server is with share one and private key. Then server identify the user from that key. Now server stacks its share two with users share one by Visual Cryptography. A new image is formed from these two images. Server will check that image with the original one while user also checks formed image with original image selected in phase one[2]. If formed image is same as original image then proceed further transaction and if it is not phishing is detected and user can terminates the transaction without any loss of confidential data[1][4].



VI. ALGORITHM

1. First load up both the host image and the image you need to hide.
2. Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.
3. Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: 10110011

4. To get the original image back you just need to know how many bits were used to store the secret image. You then

scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

Host Pixel: 10110011
Bits used: 4
New Image: 00110000

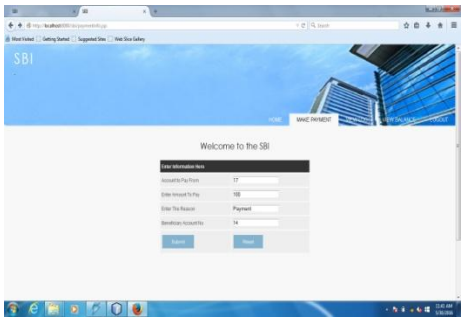
Hiding depends on the settings you choose - but as an example if we hide in the 2 least significant bits then, we can hide:

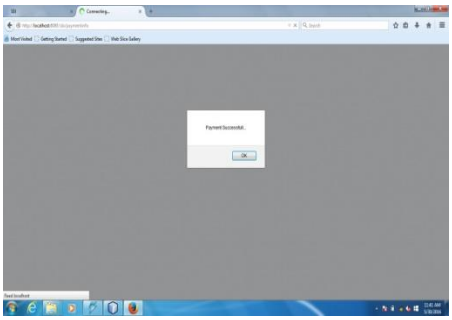
MaxBytes = (image.height() * image.width() * 3 * 2) /8

i.e. the number of pixels, times the number of colours (3), times the number of bits to hide in, all divided by 8 to get the number of bytes. It helps to hide a bit less than this because the algorithms may take a while to find places that haven't had anything hidden in it when we are close to the threshold

VII.RESULT

2. After applying Antiphishing framework:





VII.FUTURE WORKS

The proposed system is highly secured so it can be used in any online transaction like banking as mentioned in this paper. Also this system can be implemented on online recharge system, online reservation system and so on. In proposed system to complete the transaction user should have the encrypted part of image that is share one, means at the time of each transaction user is going to upload a image. To overcome such a problem we can provide alternating system to user by storing user share to server database only. And at the time of any transaction user will select one image given by the application server to user.

VIII.CONCLUSION

Phishing websites as well as human user can be easily identified using our proposed “An Anti-Phishing Framework Using Visual Cryptography” method. The proposed methodology preserved confidential information of user by using image share security. If the website is phishing web site then in that situation, the website can’t generate original image for that specific user how wants to do transaction. The proposed methodology is also useful to prevent the attack on financial web portals, banking portal, e-commerce, online shopping, etc. Zero false positives and 100% true positives are generated by using our propose mechanism for detecting and preventing phishing attacks. The results reveal that the proposed anti-phishing scheme is effective and can be used in real time applications.

REFERENCES

[1] Divyajames and Mintu Philip, A novel anti phishing framework based on Visual cryptography,978-1-4673-0449-8/12/$31.00©2012 IEEE.

[2] N.Askari, H.M. Heys and C.R.Moloney, An extended visual cryptography scheme for halftone images,2013 26thIEEE CCECE,978-1-4799-0033-6/13/$31.00©2013 IEEE

[3]Y.YesuJyothi,D.Srinivas,K.govindaraju, The secured anti phishing approach using image based validation,IJRCCT,Vol. 2,Issue 9,Sept 2013.

[4]K.A.Aravind,R.MuthuVenkataKrishnan, Anti-phishing framework for banking based on visual cryptography, IJCSMA , Vol. 2,Issue 1,Jan 2014, pg.121-126.

[5] MounikaReddy.M and MadhuraVani.B,, A novel anti phishing framework based on Visual cryptography, IJARCCE, Vol. 2,Issue 9, Sept 2013.

[6] Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method'", in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.

[7] Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE-Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.

[8] Nourian, A.; Ishtiaq, S.; Maheswaran, M.;" CASTLE: A social framework for collaborative antiphishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing:Networking, Applications and Worksharing, 2009.

