Visual Cryptography Implementation with Key Sharing For Effective Phishing Detection Process

[1]B. K. Prasath, [2] P. Ashok Kumar,
[1]*Student, Computer Science & Engineering, Ganadipathy Tulsi's Jain Engineering College,*
[2]*Student, Computer Science & Engineering, Kingston engineering college,*

Abstract: *The advent of the internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal, confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Fake websites which appear very similar to the original ones are being hosted to achieve the effective phishing detection The result shows that if we focus on user also know using a website genuine or not, we can detect genuine site to avoid wasting network resources.*

Keywords: *Phishing, Attacks, Genuine site, Half image, Half key.*

I. Introduction

Online transactions are nowadays becoming 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 in order to make it effective preventive mechanisms should can also be implemented. Thus the security in these cases is very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware have improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. So here introduces a new method which can be used as a safe way against phishing in this approach website cross verifies its own identity and Proves that it is a genuine website (to use bank transaction, E-commerce and online booking system Etc.) before the end users and make the both the sides of the system secure as well as an authenticated one. 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. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image and key sharing is once the user logged out after accessing their account, a dynamic password will be generated and send as an SMS to the mobile user. When the user logs in next time, they have to provide the new password share. By using this technique we can avoid the hacking process. Also, if some unauthorized person is accessing your account they will not be able to retrieve your account's password. This will provide more security.

II. Overview of Effective Process

When a user using the website user also known as that particular website are genuine or not, so we are making a new approach using login time and each and every transaction time. So we implement the process named as visual cryptography and session key generation process. We also implement an image based authentication using Visual Cryptography. The use of visual cryptography is explored to preserve the privacy of an image by decomposing the original image into two shares one share to an original server another share to a user to his registered e-mail. In the MODIFICATION, once the user logged out after accessing their account, a dynamic password one time password (OTP) will be generated by a genuine site which will provide to the user through a message in the registered mobile number. A half key identification technique that means the random key will provide to the valid user. This provides that the website is authenticated. When the user logs in next time, they have to provide the new password share. By using randomness algorithm phishing issues avoided. Also, if any unauthorized person accessing into your account, they will not be able to manage your accounts this technique will provide more security from the hackers.

III. Architecture Diagram

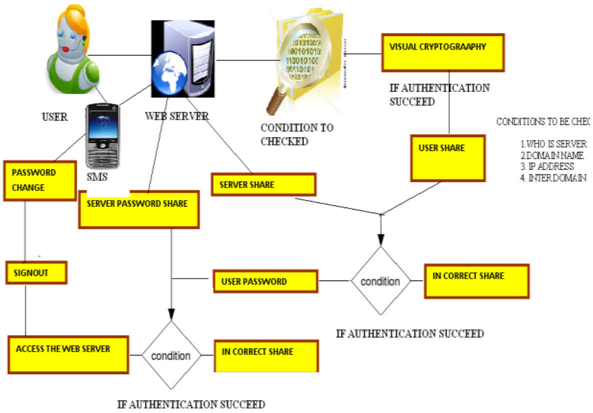

Fig1: overview of concept diagram

IV. Related Work

A. Network Construction

The network has more number of nodes. It maintains the connection details. Nodes are interconnected and exchange the data directly with each other node. Network server Store the data like IP Address, port details, nodes and status of the user. Node gives request to the server and gets the needed response from server. To construct the network, first we have to provide the number connected to the server. Once the initialized, the nodes are logged into the system.

B. Client:

This module places a vital role in this project because this is deviating from the normal registration process. Because in this module the client will register all his authentication information along with his username, password, gender, Mobile number, Age, DOB, Address. All the information is stored in the Main Server for Authentication.

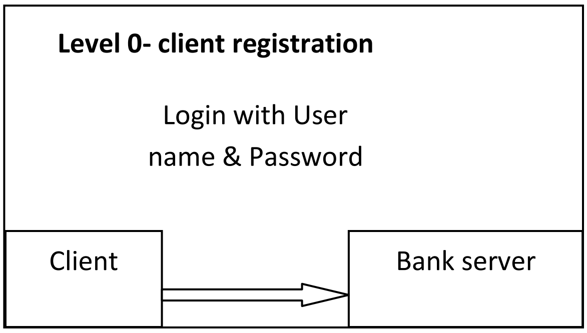

Fig 2: client server connection

C. Server

A server is a computer program running to serve the requests of other programs, the "clients". Thus, the "server" performs some computational task on behalf of "clients". The clients either run on the same computer or connect through the network. Here is the server acting as a platform to run the client request. The server is responsible for maintaining all the client information. The server will prevent the unwanted users entering into the network. It also verifies the access privileges of each and every user. The users have to be in their limits.

D. Visual Cryptography

A computer to decrypt secret Is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recover soon urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Visual cryptography (VC), A method for protecting image-based secrets that have a computation-free decryption process. In the (2, 2) VC scheme, each secret image is divided into two share such that no information can be reconstructed from any single share of image. Each share is printed on transparencies. The decryption process is performed by stacking the two shares and the secret image can be visualized by the naked eye without any complex cryptographic computations. In the above basic VC scheme, each pixel ‘p’ of the secret image is encrypted into a pair of sub pixels in each of the two shares. If ‘p’ is white, one of the two column sunderthewhitepixelinFig.1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has a 50 % probability to be chosen.

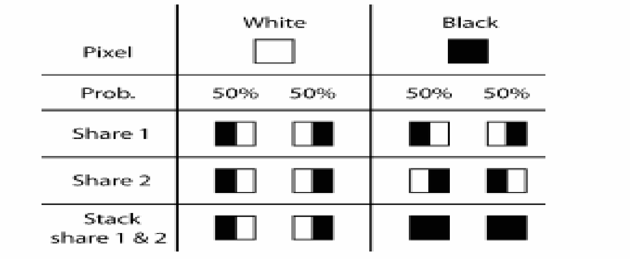

Fig 3: Construction of (2,2) VC Scheme

Then, the first two pairs of sub pixels in the selected column are assigned toshare1andshare 2, respectively. Since, in each share, picture encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image. By stacking the two shares as shown in the last row of Fig.3, if ‘p’ is white it always outputs some black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If ‘p’ is black, it outputs two black sub pixels. Hence there is a contrast loss in the reconstructed image. However the decrypted image is visible to the naked eye since human visual system averages their individual black–white combinations.

E. Session Key Generation

After verifying all the details and if it has success result means we are generating one Session key and the key will be sent as an SMS to that customer. If the customer is entered the same session key means, then only the website will be opened.

F. Authentication

Each time when the user logging the site, a new key will be generated and send to the user registered mobile number. When the user logs into the site next time, they need to provide one half of the session key and the server will provide the next half of the session. Once it was matched the user is allowed to perform the transaction. By implementing this module, the user can identify the site is original or Phishing site.

G. Transaction

The client further initializes the transaction by session login. This module provides banking functionalities to authenticated end user or client. Client can access the required functionalities of this application. Client can access balance inquiry, and also perform monetary transactions in a secured way from online banking.

- Perform transaction
- Balance Enquiry

F. Validation Of Website Phising Site

The main DNS server is having all the information about Original & Phishing Web sites. Each web site has who is information along with the IP address. WHOIS is all about the website registration, name to whom the web site is registered, along with the company details. Every Web site has an IP address, which will be used for authentication. Phishing Database is always updated with the Phishing Website’s details for verification.

The DNS server will also have the complete details regarding the Domain Name & an entire domain in the web address. Each & every website will have Domain name (.Com, .Co.in, .Edu,. Tech, .Co.uk, .in, Org &etc.). Inter domain is all about any two domain names in the same link,www.123.com/456.com. Phishing Database is always updated with the Phishing Website’s details for verification.

V Structure Of Our Proposal

The main purpose of this approach is a user using the website user also known as that particular website are genuine or not. Here new approach handles here on login time and each and every transaction time visual cryptography are image based. The use of visual cryptography is explored to preserve the privacy of an image by decomposing the original image into two shares one share to an original server another share to a user.

A user shares will be sent to a registered email address because no external drivers are supported in some computer.

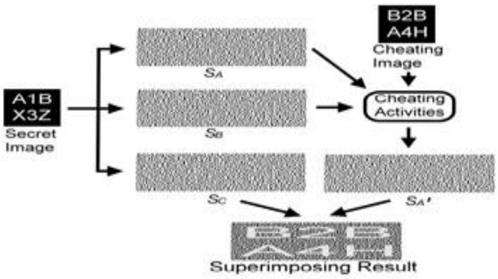

Fig 4: visual cryptography

In session key generation a new approach implementation on verifying server, which is used genuine or not they are valid user get the verification code when the user entered first half key correctly the web page will shows second half (8 digit verification code mean we will enter first 4 digits only) into that web page first half only if the code is corrected second half server will show now user also consider this is a genuine site.

V. Conclusion

In this proposal, we compare the requested site to the WHOIS server to validate whether the site is a registered one or not. WHOIS stores entire LUI information rather than only a URL of a web site in the whitelist to provide a more secure environment, Especially it can efficiently defend the harming. Moreover, authentication server contains the whitelist for the user. As our experiment shows, WHOIS identities a successful login process efficiently; unfortunately if the user entered into a phishing site, they can't miss use their detail because of additional authentication like token number. The warnings to the user will be more and more accurate.

Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified. The proposed methodology preserves confidential information of users using 3 layers of security. First layer verifies whether the website is a genuine/secure web site or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website, but not the secure website), then in that situation, the phishing website can't display the image for that specific user (who wants to log in into the website) due to the fact that the image is generated by the stacking of two shares, one by the user and the other with the actual database of the website.

References

[1] S. Stamm, Z. Ramzan, et Jakobsson Markus, "Drive-By Pharming," Proceedings of the 9th international conference on Information and communications security, Zhengzhou, China: ACM, 2007, p. 495-506.

[2] G. Ollman, "The Pharming Guide," Jul. 2005; http://www.ngssoftware.com/papers/ThePharmingGuide.pdf.

[3] C. Jackson, A. Barth, A. Botz, W. Shao, et D. Boneh, "Protecting browsers from DNS rebinding attacks," ACM, vol. 3, Issue 1, Jan. 2009.

[4] C. Karlof, U. Shankar, J. Tygar, et D. Wagner, "Dynamic pharming attacks and locked same-origin policies for web browsers," Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Viriginia, USA: ACM, 2007, p. 58-71.

[5] S. Egelman, L. Cranor, et J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, Florence, Italy: ACM, 2008, p. 1065-1074.

[6] Y. Cao, W. Han, et Y. Le, "Anti-phishing Based on Automated Individual White-List," Proceedings of the 4th ACM workshop on Digital identity management, Alexandria, Viriginia, USA: ACM, 2008, p. 51-60.

[7] M. Hara, A. Yamada, et Y. Miyake, "Visual similarity-based phishing detection without victim site information," Nashville, Tennessee, USA: IEEE, 2009, p. 30-36.

[8] A.P.E. Rosiello, E. Kirda, C. Kruegel, et F. Ferrandi, "A layoutsimilarity- based approach for detecting phishing pages," Nice, France: IEEE, 2007, p. 454-463.

[9] E. Medvet, E. Kirda, et C. Kruegel, "Visual-Similarity-Based Phishing Detection," Proceedings of the 4th international conference on Security and privacy in communication networks, Istanbul, Turkey: ACM, 2008, p. Article No. 22.

[10] W.B. Cavnar et J.M. Trenkle, "N-Gram-Based Text Categorization," Proceedings of SDAIR, 1994.

[11] E.W. Myers, "An O(ND) Difference Algorithm and Its Variations."

[12] S. Wu, U. Manber, G. Myers, et W. Miller, "An O(NP) sequence comparison algorithm," Information Processing Letters, Sep. 1990, p. 317-323.

[13] Phishtank, "PhishTank home"; http://www.phishtank.com/.