IJCSN International Journal of Computer Science and Network, Volume 3, Issue 2, April 2014
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.274

Image Based Authentication for Phishing using Visual Cryptography

[1] Ritika Ogra, [2] Niharika Limaye, [3] Vrushali Deshmukh

[1, 2, 3] Department of Information Technology, VIIT
Pune, Maharashtra 411048, India

Abstract - With the advent of internet, various online attacks have 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 this. In this paper we have proposed a new approach named as an "Image based authentication using Visual Cryptography" to solve the problem of phishing. The use of visual cryptography is explored to preserve the privacy of an image by decomposing the original image into two shares (one with user and one with server) such that the original image can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image. Using this website cross verifies its identity and proves that it is a genuine website before the end users. The emphasis of the project is to prevent the user from visiting a phishing website. The project aims at achievement of security of user and saving its confidential information from theft.

Keywords - *Phishing, visual cryptography, image, shares, security.*

1. Introduction

Phishing attacks are increasing in frequency and sophistication. The Anti-Phishing Working Group (APWG) recently reported that the number of attacks is growing by 50 percent per month, with roughly 5 percent of recipients falling victim to them. Phishing Web pages generally use similar page layouts, styles (font families, sizes, and so on), key regions, and blocks to mimic genuine pages in an effort to convince Internet users to divulge personal information, such as bank account numbers and passwords. Now days everyone do online transactions which has become very common. In this type of transactions various attacks takes place, phishing is occurred as a major security threat and various new ideas are implemented so to avoid this some preventive mechanism should be implemented .Thus the security in these cases should be very high and should not be easily traceable. Hence it is very hard that whether a computer that is connected to the internet can be considered trustworthy and is secure or not. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. One definition of phishing is given as "it is a criminal activity using social engineering techniques. Phishes attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication".

We are proposing a technique in which Image processing is used which is used to divide the image into shares such that stacking of shares reveals the original information. The cryptographic algorithm and Deffie Hellman key exchange is used for encryption and decryption of shares. By using the cryptography the image share which is used to prevent Phishing is secretly encrypted and sent to trusted server such that the server under test if legitimate will reveal original image on decryption and the phished website gets detected because it does not reveal the original image on decryption.

2. Literature Survey

This section includes the work already done on this system by various researchers using different methodologies and algorithms. Following is the brief description of some of them:

2.1 DNS Based Anti Phishing Approach

This method was proposed by

[1].Blacklist is a DNS based anti-phishing approach technique now most commonly used by the browser. Anti Phishing Work Group, Google and other organizations have provided an open blacklist query interface. Internet Explorer7, Netscape Browser8.1, Google Safe Browsing (a feature of the Google Toolbar for Firefox) are important

browsers which use blacklists to protect users. In this technique every URL in the blacklist has been verified by the administrator, the false alarm probability is very low. Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database.

2.2 LARX Based Detection

This paper is proposed by Tianyang Li.; Fuye Han.; Shuai Ding and Zhen Chen. An offline phishing detection system named LARX, acronym for Large-scale Anti-phishing by Retrospective data-exploration [2] to counter phishing attacks has been proposed. First, it uses traffic archiving in a vantage point to collect network trace. Secondly, LARX leverage cloud computing technology to analyze the experimental data in a way similar to the divide and conquer scheme. It used two existing cloud platforms, Amazon Web Services and Eucalyptus. A physical server is also used for comparison. All of LARXs phishing operations are based on a cloud computing platform and work in parallel. The disadvantage is that is it used, as an offline solution but LARX can be effectively scaled up to analyze a large volume of network trace data for phishing attack detection.

2.3 Visual Similarity Assessment method

This paper is proposed by Liu Wenyin and Anthony Y. Fu etc. [3]. A page visual similarity assessment method to detect phishing websites, if a web page is similar to a financial organization's page, but it is not the organization's web page itself; it is considered a phishing site's page. Jung Min Kang and Do Hon. Lee [4] proposed the URL similarity assessment method, if an URL is similar to a bank's URL, but it is not the bank's URL, it is considered a phishing website's URL. There is low assess accuracy rate for the URL and content similarity assessment techniques.
The speed of calculating the visual similarity between pages is too slow, so it is only used for phishing-spam detection generally.

2.4 Heuristic Based Anti Phishing approach

This paper is proposed by Nourian, A.; Ishtiaq, S.; Maheswaran, Heuristic based anti-phishing technique is to estimate whether a page has some phishing heuristics characteristics. For example, some heuristics characteristics used by the Spoof Guard [5] toolbar include checking the host name, checking the URL for common spoofing techniques, and checking against previously seen images. If you only use the Heuristic-based technique, the accuracy is not enough. Besides, phishes can use some strategies to avoid such detection rules.

2.5 Observed Failures in Previous Systems

1) Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database.
2) Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to use technical means to avoid the heuristic characteristics detection.
3) Similarity assessment based technique is time-consuming. It needs too long time to calculate a pair of pages.

3. Current Scenario

In the current scenario as shown in the Fig. 1, when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. On the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such 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.

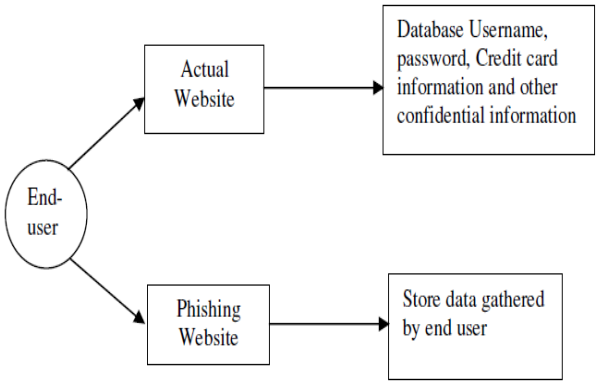


Figure1: Current Situation

4. Proposed Methodology

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

The proposed approach can be divided into two phases:

A. Registration Phase
B. Share Generation
C. Verification Phase

A. Registration Phase

During the registration process the client registers itself at the trusted server i.e. (For e.g.: bank) and enters the registration details like name, address, mobile no etc which Gets stored at the trusted server database. The key pair is Generated at the client side. The trusted server stores the key

Pair and user id details. This is used further for encryption and decryption process. The user is provided with the option to update his keys using the Deffie Hellman key exchange process. So as to use the keys securely. .

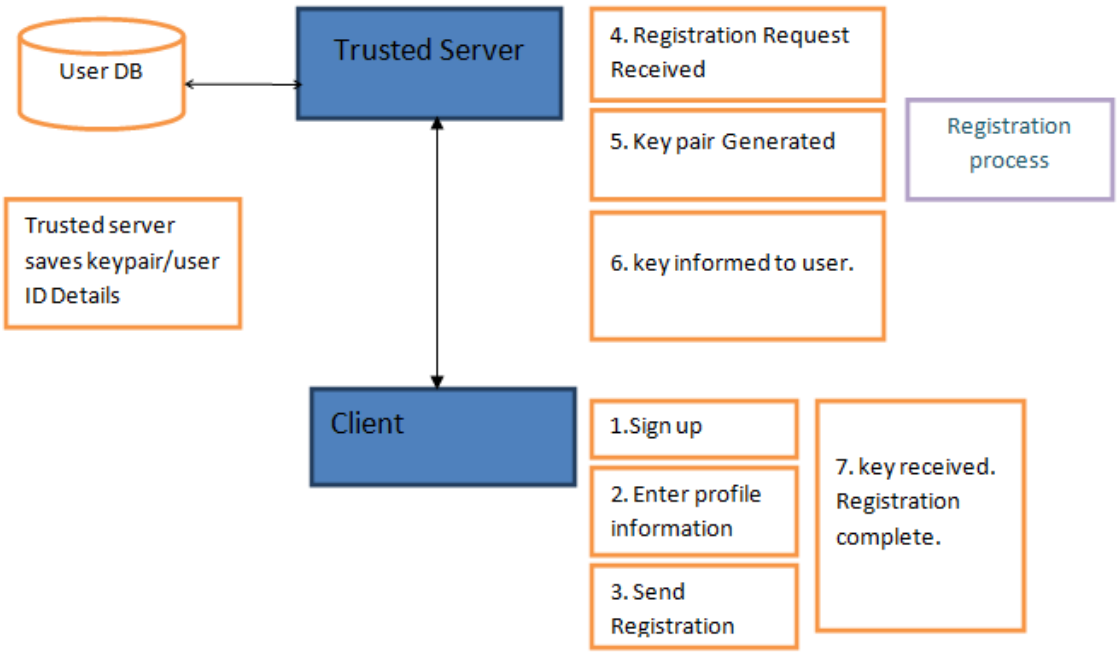


Figure 2: Registration process

B. Share Generation

During the verification process the client will load The image randomly which gets resized into 200* 200. The image is the grayscale so as to convert the 24 Bit image into 8 bit image by extracting the RGB value of the pixels. The gray scaling image is converted into And white image using threshold algorithm of image Processing. The black and white image has a pixel value Of 0 and 1. The visual Cryptography scheme by Nair Shamir is further used for share generation. Using the VCS scheme [6] randomly matrix are generated in share1 Part of image using random function. Each pixel is Then checked with the pixel value. Such that if pixel Value=0 then matrix in share1 gets as it's copied in
Share2 and if pixel value=1 then matrix bits are inversed. The stacking process is that these 2 shares are
Then compared such that if its is same matrix the pixel Value=0 otherwise1.This reveals the original image

C. Verification Phase

In this phase the webpage is verified if it is legitimate Or not. The shares done during share generation phase Are now used for verification of server. The share 1 is Then encrypted using the keys. This share1 gets ransmitted using keys to server under test. The server under test gets

the encrypted share from client and then retransmits the share to trusted server. The user id and the share1 in encrypted form are transmitted to trusted server. The decryption of server is done only if the server under test is registered with the trusted server. If it has then trusted server provides the decrypted version of share. This decrypted version is then used to reveal the original image. The DES cryptographic algorithm is used for the encryption and decryption of shares. The DES algorithm uses 64 bit key and is good cryptographic algorithm used for security. The original image gets generated from new share1 and old share2. The user has to check if the image is similar to loaded image. If it is then the server is verified otherwise it is a phished server.

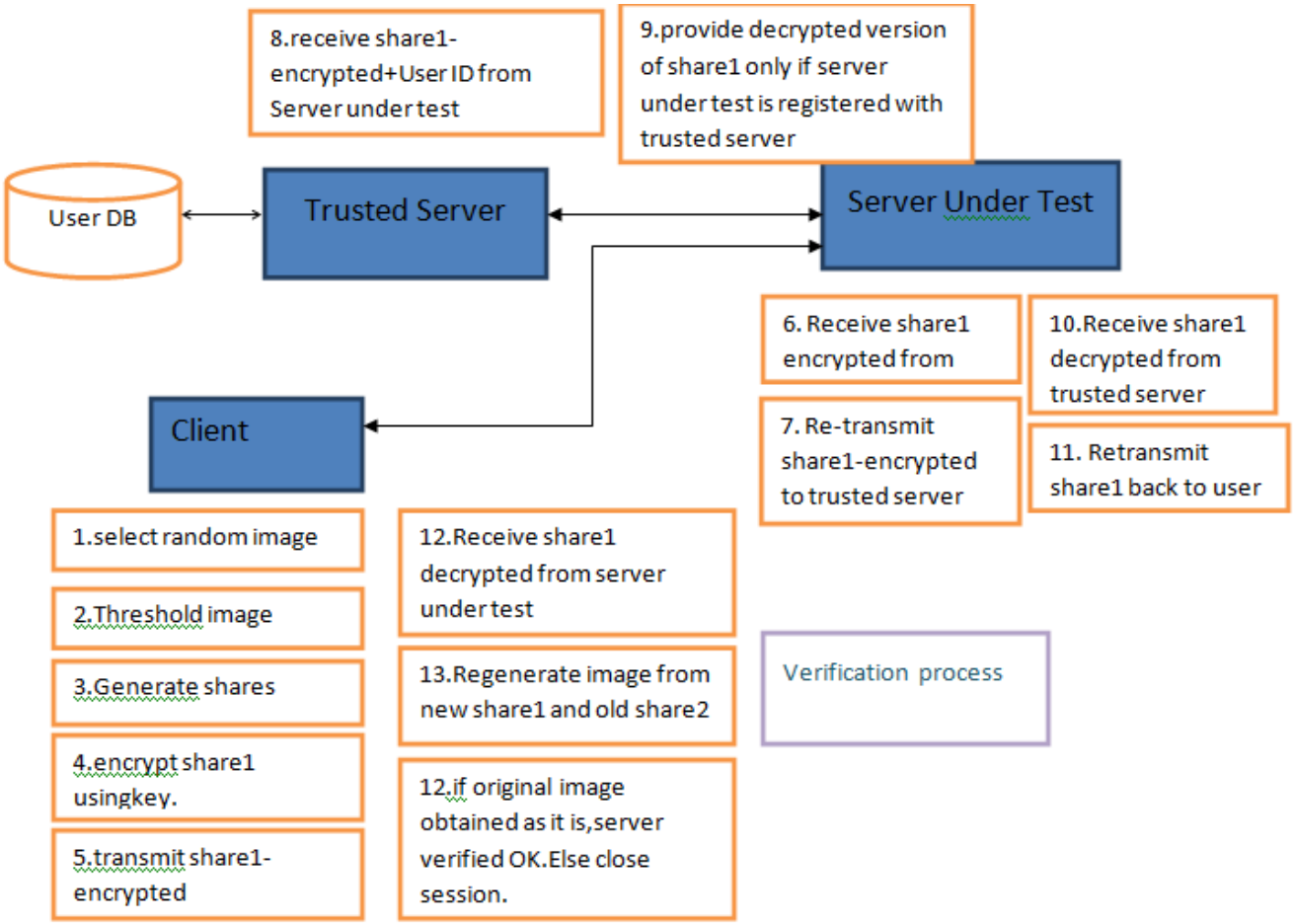


Figure 3: Verification Process

5. Implementation and Analysis

The proposed methodology is implemented using java. During the verification process the important part is the loading of image and then creation of shares for that image. The image shares are then stacked over to reveal the original image.The image is used to verify whether the server is original or not.

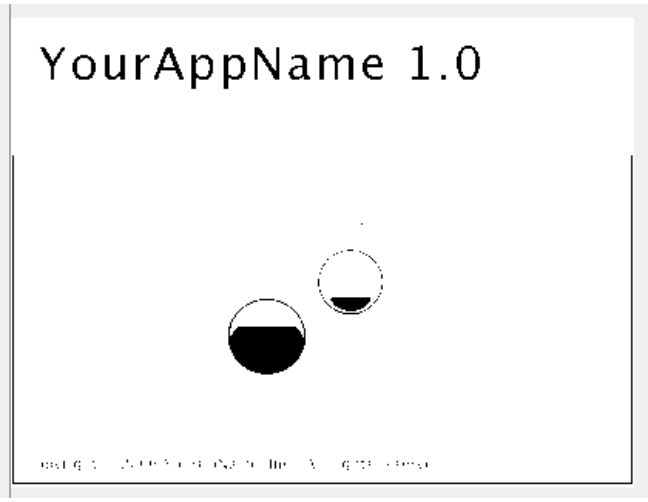
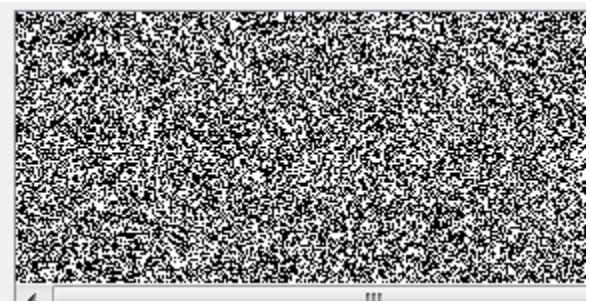
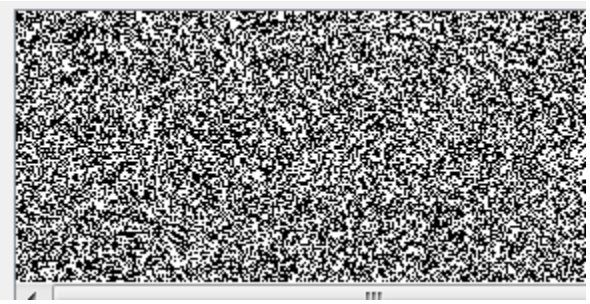


Figure 4:Original image



Share 1



Share 2

Figure 5: Creation and stacking of shares

6. Future Scope

This system can be implemented further by using a certain 'process' button wherein the system will be designed in such a way that the trusted server itself will detect whether the server under test is trusthworthy or not. This can be done with the help of the process which will consist of the image processing algorithms and visual cryptography coding such that when the button gets clicked the server is tested.

Another way can be, the other cryptography algorithms can also be used for the verification.

7. Conclusion

Currently phishing attacks are so common because it can attack globally and capture and store the user's 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 using our proposed "Image based Authentication Based on Visual cryptography". It verifies whether the website is a genuine/secure website 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. It also verifies whether the user is a legitimate user or not with the help of the key.

Acknowledgments

An endeavor is successful only when it is carried out under proper guidance & blessings. We would like to thank people who helped us in carrying out this work by lending invaluable assistance to us in carrying out this work. We are hereby thankful to Prof. Mr. S.R. Sakhare, Head of Department, Information Technology, VIIT, Pune & Prof. Mr. Narendra Pathak, Project Coordinator, Department of Information Technology, VIIT, Pune who encouraged at this venture. We sincerely thank Prof. Mrs. L.A. Kamble, Project Guide, VIIT, Pune for their constructive & encouraging suggestions. We also thank all Teaching and Non-teaching staff of Department of Information Technology, VIIT, Pune for their kind of co-operation during our course. Finally we are extremely thankful to our Family & Friends who helped us in our work & made the project a successful one.

References

[1] "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010".

[2] " Tianyang Li.; Fuye Han.; Shuai Ding and Zhen Chen.; "LARX: Large-scale Anti-phishing by Retrospective Data-Exploring Based on a Cloud Computing Platform", in Proceedings of IEEE- 20th International Conference on Computer Communications and Networks, 2011.

[3] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)".

[4] "CASTLE: A social framework for collaborative ant phishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing: Networking, Applications and Work sharing, 2009.

[5] "New Ant phishing Method with Two Types of Passwords in Open ID System", in Proceedings of IEEE Fifth International Conference on Genetic and Evolutionary Computing, 2011.

[6] M. Nair and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994.