International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

ONLINE TRANSACTION PROTECTION WITH DUAL IMAGE OVERLAPPING FOR PHISHING WEBSITE

Parameswari.A[1], Mathumitha.D.G[2], Janani.M[3],Preethi.A.R[4]

[1,2,3,4] *Dept of IT, Jeppiaar SRR Engineering College, Tamil Nadu, India.*

Abstract - *Phishing is an attempt by a group or an individual to thieve personal confidential information such as password, credit card number etc from unsuspecting victims for financial gain, identity hacking and other fraudulent activities. The first defense should be strengthening the authentication mechanism in a web application. For web sites providing critical financial transactions a simple username and password based authentication is not sufficient. In this paper we have proposed a new approach to solve the problem of phishing. The original image captcha is decomposed into two shares to preserve the privacy of the image captcha. They are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available. The individual sheet images can not reveal the identity of the original image captcha. Once the original image captcha is revealed it can be used as the password by the user. Several solutions have been proposed to tackle phishing attack.*

***Key Words**: NetBeans, MySQL.*

1. INTRODUCTION

Nowadays online transactions become very common and there are various attacks present behind this. Among 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. Thus the security should be very high and should not be easily tractable with implementation and today most applications are only as secure as their underlying system. Their detection is a difficult problem since the design and technology of middleware has improved steadily. Phishing scams are also becoming a problem to online banking and e-commerce users. The question is how to handle high level of security applications. Phishing is a criminal activity using social engineering techniques. Identity theft can be described as “a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain”. Phishing attacks are based on technical deceit and social engineering practices. The most successful phishing attacks have been initiated by email – where the phisher impersonates the sending authority so here introduces a new method against phishing which is named as "A novel approach against Anti-phishing using visual cryptography". Website cross verifies its own identity and proves that it is a genuine website 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 that an input image is processed to get the improved form of the same image and/or characteristics of the input image. Visual Cryptography is a method of encrypting a secret image to shares, such that overlapping a sufficient number of shares reveals the original secret image.

2. PROBLEM IDENTIFIED

Phishing web pages are forged web pages to mimic web pages of real web sites that are created by malicious people. Those web pages look exactly like the real ones and victims of phishing web pages may expose their bank account details, password, credit card number, or other important information to the owners of phishing web page. It includes techniques such as tricking customers through email and spam messages, installation of key loggers, man in the middle attacks and screen captures. Blacklist-based technique with low false alarm probability, it detects the websites that are in the blacklist database because the life cycle of phishing websites is too short and the blacklist accuracy is not too high. Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to avoid the heuristic characteristics detection by using technical means. Similarity assessment based technique is time-consuming and needs too long time to calculate a pair of pages.

3. PROPOSED MODEL

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. (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. In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares 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. 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. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

4. PROPOSED DIAGRAM

The proposed model block diagram is represented as follows:

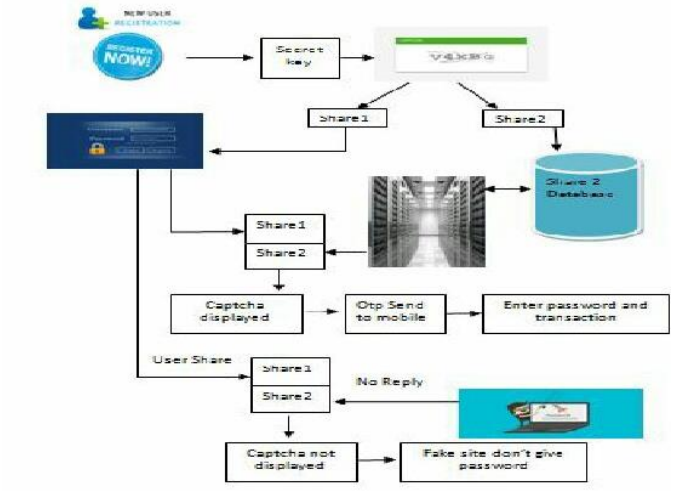

Figure1: Architecture Diagram

4.1. BLOCK DIAGRAM EXPLANATION

First register the entire details, it will be stored into the database and a 8-bit secret key is randomly generated. After registration process, the user's secret key and randomly generated secret key is combined and converted into an image using BufferedImage and Graphics2D java classes. The image is encrypted using visual cryptography and the image captcha is generated. Each pixel is divided using splitting and rotating algorithm and separately stored in share1 and share2.The share1 is downloaded by the user and share2 is stored in the bank server. If the user wants to login, they have to upload the share1 image then the validation process is done. The share1 image from the user and the share2 image from the bank server are superimposed and if the original image is revealed then the OTP is send to the user's mobile. The original image captcha is displayed and the user has to enter the correct password and login into their account. Further process like deposit, withdrawal, transaction procedures are done. If the user doesn't have the share1 image, he doesn't able to access the site and further process can't be proceeded.

5. MODULES DESCRIPTION

5.1. REGISTRATION WITH SECRETE CODE

In the registration phase, the user details along with a key string are asked from the user at the time of registration. The key string can be a combination of 8-bit alphabets and numbers to provide more secure environment. This string is concatenated with 8-bit randomly generated string in the server. The random string is generated using Blowfish Algorithm. Blowfish Algorithm is a type of Random Algorithm by which random strings can be created.

5.2. IMAGE CAPTCHA GENERATION

A key string is converted into image using java classes Buffered Image and Graphics2D. The dimension of the image is 260*60. Text color is black and the background color is white. Text font is set by java class Font. The image is encrypted using visual cryptography and the image captcha is generated. The image will be divided into many pixels. After image generation it will be written into the user key folder in the server using ImageIO class.

5.3. SHARES CREACTION (VCS)

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. We use Splitting and Rotating algorithm for dividing the image captcha. During login phase the user's share and the original image captcha are sent to the user for later verification. The image captcha is also stored in the actual database of any confidential website as confidential data.

5.4. LOGIN

In the login phase one of the username and the user share from the user is uploaded. The share1 image from the user and the share2 image from the bank server are superimposed and if the original image is revealed then the OTP is send to the user's mobile. The original image captcha is displayed and the user have to enter the correct password and must upload the OPT, it will check with the OPT in database and after it matches the account number is generated. Further process like deposit, withdrawal, transaction procedures are done.

6. TECHNIQUES USED

6.1. NETWORK SECURITY

Network security consists of the policies and practices adopted to monitor and prevent unauthorized access of data and confidential information, misuse, modification, or denial of service and network accessible resource. Network security starts with Authentication, commonly associated with a username and a password or other

authenticating information that allows them access to confidential information and programs within their authority. Network security covers both public and private network. That is used in every field i.e. everyday jobs, conducting communication and transaction in businesses, individuals and government agencies.

CODING LANGUAGES

JAVA

A platform is the hardware or software environment in which a program runs. The Java platform differs from other platforms that it is a software-only platform that runs on top of hardware-based platforms. Normally most of the other platforms are described as a combination of hardware and operating system. The Java platform has two components they are the Java Virtual Machine and Java Application Programming Interface .It's the base for the Java platform and is ported onto various hardware-based platforms. The Java API has a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface widgets, bufferedimage. The Java API is grouped into libraries of related components.

RESULTS AND DISCUSSION

CONCLUSIONS

Currently phishing attacks are so common because it can attack users globally and capture and store the users' confidential information. This information is gained and used by the attackers which are indirectly involved in the phishing process. Using our proposed method "Anti-phishing framework based on Visual Cryptography" phishing websites as well as human users can be easily identified. The proposed methodology secures confidential information of user and 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 created by phisher), then in that situation, the phishing website can't display the image captcha for that specific user (who wants to log in into the website like original user) due to the fact that the image captcha is generated by the stacking of two shares, one is with the user and the other is in the actual database of the website. The proposed technique is also useful to tackle the attacks of phishing websites on financial web portal, online banking, and online shopping market.

6. REFERENCES

[1]Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, and K.-W. Wong, "Chosen plaintext attack of an image encryption scheme based on modified permutation–diffusion structure," Nonlin. Dyn., vol. 84, no. 4, pp. 2241–2250, 2016.

[2]A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 235–246, Feb. 2016.

[3]Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," IEEE Trans. Cybern., vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[4]Y.-G. Yang, Q.-X. Pan, S.-J. Sun, and P. Xu, "Novel image encryption based on quantum walks," Sci. Rep., vol. 5, no. 7, 2015, Art. no. 7784.

[5]H. Zhu, C. Zhao, X. Zhang, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," Optik Int. J. Light Electron Opt., vol. 125, no. 22, pp. 6672–6677, 2014.

[6]Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-gray code for image systems," IEEE Trans. Cybern., vol. 43, no. 2, pp. 515–529, Apr. 2013.

[7]H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Opt. Commun., vol. 284, nos. 16–17, pp. 3895–3903, 2011.

.