IJCTA, 10(02), 2017, pp. 7-12

A Survey on Phishing Attack in Internet

A. Jayanthi* D. Daya Florance* A. Merry Ida* W. Ancy Breen* and R. Anto Rose*

Abstract : Phishing is an aim of an individual or a group of persons to thieve sensitive information like passwords, credit card details etc from victims for identity theft, financial gain and other fraudulent activities. In our project we have proposed a new method that is used to solve the problem of phishing and to distinguish phishing site from legitimate sites. Phishing websites consists of a variety of cues within its content-parts as well as the browser-based security indicators provided along with the website which we say as Captcha as graphical passwords (CaRP). CaRP is a combination of Captcha and a graphical password scheme. The images is Used to protect the privacy of image captcha by dividing the original image captcha into two shares. One share will be stored in the server and another share will be provided to the user .The original image captcha will be shown only when both of these shares are overlaid, the individual images do not reveal the identity of the original image captcha. Once the original image captcha is visible to the user it can be used as the password for the user.

Keywords : visual cryptography, visual secret sharing,halftone technique, image processing.

1. INTRODUCTION

Online transactions are nowadays very common and there are several attacks present behind this. There are various attacks present so phishing is considered as a major security danger and many innovative ideas are arising nowadays for obtaining sensitive information with this in each second so preventive mechanisms should be considered and those mechanisms should also be effective.

Thus the security in these types is very high and it cannot be easily tractable with the implementation easiness. There are many applications nowadays are being very secure because of their underlying system. The design of the middle ware is improved steadily so their detection is difficult.

As a result, it is considered to be impossible for the users to be sure whether a computer that is being connected to the internet is secure or not. Phishing scams are becoming problem for the people who use online banking and e-commerce. Therefore the question arises between the users how to handle those applications that require a high level of security.

Phishing is theft which is done in online by malicious people in order to obtain the most important and sensitive information. The sensitive information which phishers are interested is confidential information such as victims password and their credit card information. The phishers aims to obtain those sensitive information by doing fraudulent activities.One of the definition of phishing is given as “it is a convict activity which is done using social engineering techniques”. Phishers aims to obtain sensitive information such as user passwords and credit card details, where the phishers act as a trustworthy person. Phishers after obtaining these sensitive information they use for their own gain with the use of technology. Phishing attacks depend upon combination of technical deceit and social engineering practices. In most of cases the phisher will make the victim to intentionally perform actions that will help them to access their confidential information.

* Assistant Professor Department of Information Technology VelTech HighTech Dr.Rangarajan Dr.Sakunthala Engineering College,Chennai, India. *jayanthiarumugamk@gmail.com, dayaflorance@gmail.com, idamerry@gmail.com, breen.cse@gmail.com, antorose@ velhightech.com*

Instant messaging services, IRC , WebPages , email are very popular. In all these cases the phisher will act like a trusted source for the user to believe. Nowadays the phishing attacks have been done by email where the phisher will get the sending authority and they will obtain the victims information through email spoofing.

"A novel [1] approach against Anti-phishing using visual cryptography" is used which acts as against anti phishing. In this method website verifies itself that it is a genuine website or not (to use bank transaction, E-commerce and online booking system etc.) and make 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 where an input image is processed to get the output which is improved form of the same image. Visual Cryptography(VC)[1][7] is a method of encrypting a secret image to shares, such that merging a sufficient number of shares will reveal the secret image.

Visual Secret Sharing (VSS) is a perfect method[3][7] that protects a secret image by dividing it into shadow images. VSS can be easily decrypted by the human visual system without the knowledge of cryptography computations.

Halftone technology [7][6] scheme is an image comprised of discrete dots rather than continuous tones. When the image is viewed from a distance, the dots will get blur together, which will create the illusion of continuous lines and shapes.

2. EXISTING SYSTEM

In [1] they noted Visual Cryptography(VC) scheme encodes the black and white secret image by using (2, *n*) threshold VCS into n shares .The reconstructed image will be darker than the background images. Threshold VC is a conventional threshold $*k* out of $*n* VCS ($*k*, $*n*). One secret image $*p* can be encoded into $*n* seemingly random transparencies such that superimposed result of any group of $*k*, while that of less than $*k* ones cannot by using integer line program.

In [2] they focused on improved VCS for secret hiding. Hiding a colored image into multiple colored cover images. Using this, generated camouflage images contain less noise compared to original clang's algorithm. Improvement in signal to noise ratio of camouflage image by producing images with similar quality to originals. Lossless recovery and reduces noise in cover images without adding additional complexity. It does not require any additional cryptographic computations. The camouflage images obtained using the modified algorithm look less susceptible of containing a secret image than ones obtained using the original method.

In [3] they used pixel encoding in VC for general access structure. It scans the secret image by zigzag and perceives a pixel block with many pixels as to encode for each run. Pixel block consists of consecutive pixels of same type during the scanning. Good quality for overlapped images and high efficiency for encoding. Suitable and adaptable for chromatic images and general access structure. It only scans the original image instead of temporarily storing the image.

Hence in [4] they also used Halftone technique for color VCS scheme using meaningful shares. VC hides the secret images into two or more images. This image can be recovered by stacking the shares together without any complex computation. This system can be combined with digital watermarking or visual verification system. Shares do not look like random noise.

In [5] they discussed VSS scheme for multiple secrets without pixel expansion. It encrypts a secret image into n share images. The secret image is revealed by printing share image on transparencies and stacking directly. Human can see secret image without any device. It can share two binary secret image on two rectangular share image with no pixel expansion. It has excellent recovery quality for secret images. It does not use codebook to encrypt secret images. Challenge of obtaining no pixel expansion in VSS has not yet resolved.

In [6] they focused on improving contrast in random grids based Visual Secret Sharing (VSS) . Random grids based (n, n) scheme, decryption is done with the help of human visual system by stacking the cipher grid. Decryption operation is done using Boolean XOR operation. VC scheme also require the generation of code book prior to share a secret image by using XOR operation. Lossless secret reconstruction.

In [7] they used Halftone technique for the journey of VCS from black to white images to colored. It merges the technology for secret sharing which allow visual information to be encrypted that decryption can be done by Human Visual System. Halftone technique achieves all the desired property. Scheme does not need to be dithering, which would degrade the quality of reconstructed image.

In [8] they used discussed on enhanced colour VSS scheme using modified error diffusion that hides information in images which divide secret images into multiple shares. Secret information can be recovered by assembling of the decrypted shares. Hiding information in images which divide secret images into multiple shares.

In [9] they mentioned Secure two party computation which involves merging together in a suitable way two beautiful ideas of circuit construction and Visual Cryptography(VC). Two party computation in presence of a static semi honest adversary. It plays a key role in secure computation. It do not follow the traditional entropy based characterization and do not play the roles they deserve.

3. PROPOSED SYSTEM

In our system Image processing and visual cryptography concepts are used . Image processing is a method of the analysis and manipulation of a digitized image, especially in order to improve its quality. Visual Cryptography (VC) is a method of decomposing an into shares and in order to reveal the original image the number of shares should be combined.

VCS is a cryptographic technique that allows for the encryption of visual information such that decrypt via sight reading. There are three vcs schemes available .We can achieve this by one of the following access structure schemes.

1. **(2, 2)- Threshold VCS scheme :** This scheme is simple which takes a secret message and then it encrypts it and provide two different shares that will only reveal the secret image when they are overlaid.
2. **(*n*, *n*) -Threshold VCS scheme :** In This scheme it takes the secret image and encrypts that to n shares such that when all n shares are combined then the secret image will be revealed.
3. **(*k*, *n*) Threshold VCS scheme :** This scheme will encrypt the secret image to n shares such that when any group of k shares are overlaid the secret image will be revealed.

In our proposed system we will use (2,2) threshold VCS scheme . In this each pixel P in the original image is encrypted into two sub pixels called shares. These two sub pixels 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). In this the Neither share provides any information about the original pixel since different pixels in the secret image will be encrypted using independent and 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 will get two black sub pixels; if it is a white pixel, we will get one black sub pixel and one white sub pixel.

In our proposed system the user registration will be done in the main server where it prompts the user to enter the secret key. These secret key consists of two sets where one set will be entered by the user and then the another set will be generated by the server. When these two sets combined together an image captcha will be created. This image captcha will consists of two shares where one share will be given to the user and another share will be saved in the server itself. When user login next time then it will prompt the user to upload the image. When the user uploads the image it should match with the image in the server and the original image captcha should be displayed. Then the one time password(OTP) will be sent to the

mail and then the user can enter their password and can make transaction. When the shares do not match then the server will not reply and then the captcha will not displayed. The user can now understand that it is fake site and do not give passwords.

4. PERFORMANCE AND LIMITATIONS

We are proposing a new method for phishing prevention. In our method an image captcha is used and validation of the image captcha is done using visual cryptography. By using this method we can protect our password and other confidential information from the phishing websites.

The emails will attract the users to make them access their fake websites created by the phishers and will intentionally make them to access that website and to expose the sensitive information.

The rapid development and evolution of phishing techniques pose a big challenge in Web identity security for computer science researchers in both academia and industry. Advanced counter measures are required in urgency. All phishing attacks spoof users from the visual level and semantic level, i.e., they make the appearances of web pages look similar to the real ones and make the web links and web page contents semantically related to the real ones.

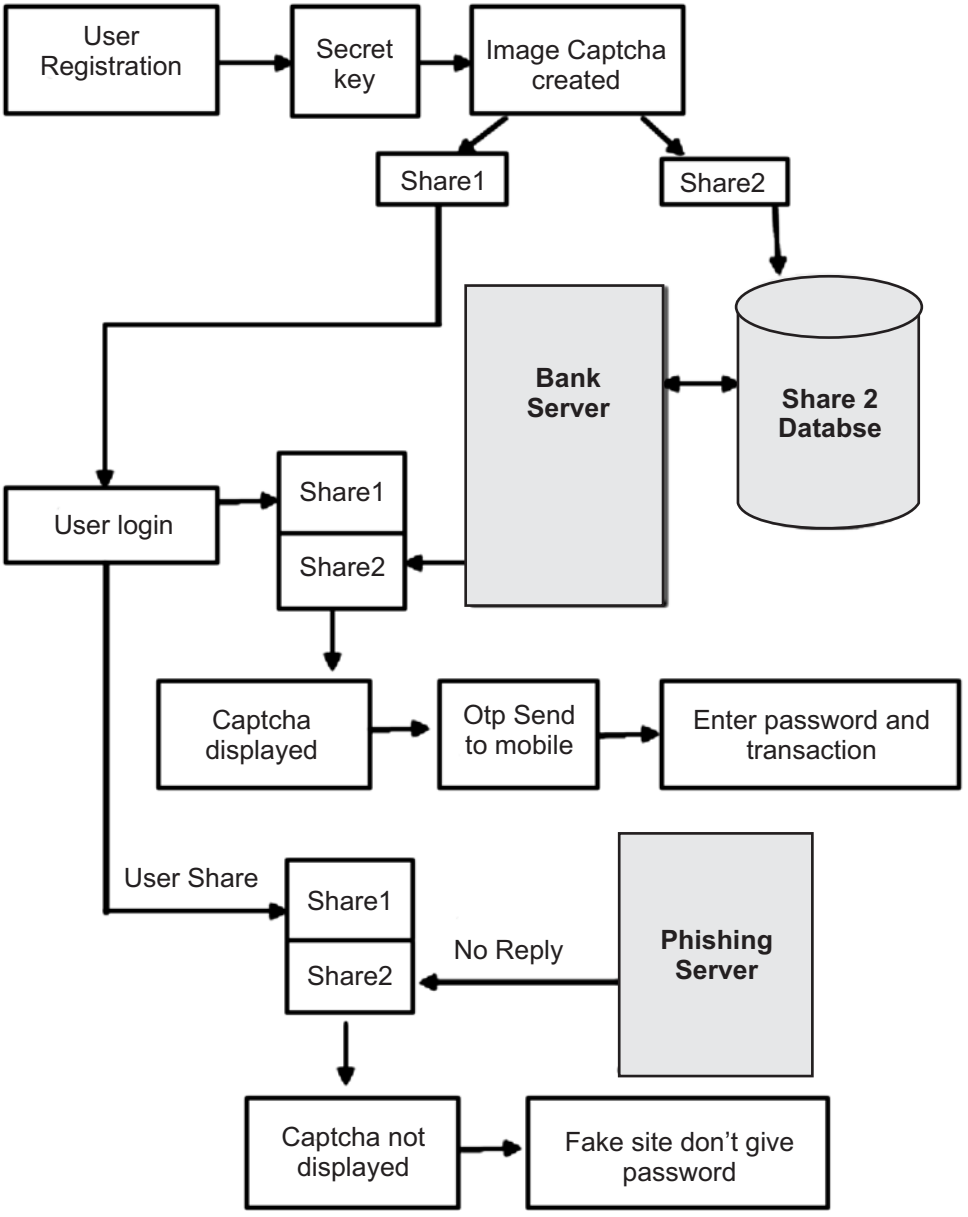

Figure 1: System Architecture

5. ADVANTAGES OF PROPOSED SYSTEM

1. 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 Captcha validation scheme using visual cryptography.
2. It prevents password and other confidential information from the phishing websites.
3. It prevents password and other confidential information from the phishing websites.
4. URL address on the address bar of your internet browser begins with “https”; the letter’s’ at the end of “https” means ‘secured’.
5. Look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Verify the security certificate by clicking on the padlock.

6. CONCLUSION

Phishing websites as well as human users can be easily identified using our proposed “Anti-phishing framework based on Visual Cryptography”. The proposed methodology preserves confidential information of users. 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 captcha for that specific user (who wants to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

7. SUGGESTED FUTURE WORK

Nowadays, Computer-generated frauds are generating forged websites same as of the original/genuine websites and hence arrest and store confidential information of the user. By using this system it is possible to overcome above situation. The system helps to recognize the website is genuine or not and if it is not thenthe confidential information of the user will not be exposed to the forged website. Using of the shared images are the security key in this system. The security level of this system is increases. This system has used in the regions like banking, finance and online shopping.

8. REFERENCES

1. C. Blundo, S. Cimato, A. De Santis, Visual cryptography schemes with optimal pixel expansion, in Cryptology ePrint Archive, Report 2006/170,2006, <http://eprint.iacr.org/2006/170>.
2. R Youmaran, A Adler, A Miri, Improved VCS for secret hiding Communications, 2006, 23rd Biennial Symposium.
3. G Ateniese, C Blundo, A De Santis ,in Journal of Computers, Vol 3, No 12 (2008), 68-75, Dec 2008.
4. HC Wu, HC Wang, RW Yu, color visual cryptography scheme using meaningful shares,in Intelligent Systems Design and Applications, 2008. ISDA ‘08. Eighth International Conference on (Volume:3) 26-28, Nov 2008.
5. TL Lin, SJ Horng, KH Lee, PL Chiu, TW Kao, Visual secret sharing scheme for multiple secrets without pixel expansion in National Science Council Volume 37, Issue 12, December 2010.
6. Sachin Kumar and R. K. Sharma, Improving Contrast in Random Grids Based Visual Secret Sharing , International Journal of Security and Its Applications Vol. 6, No. 1,January, 2012.
7. N Gupta, M Gupta, A Mishra, Journey of VCS from Black and White Images to Colored Images with their Performance Analysis , in International Journal of Computer Applications (0975 – 8887) Volume 79 – No9, October 2013.
8. Joseph James S and Rajan S , Enhanced Color Visual Secret Sharing Scheme using Modified Error Diffusion,in International Conference on Research Trends in Computer Technologies 2013 ICRTCT(2):25-29, February 2013.
9. Paolo D’Arco , Roberto De Prisco, Secure two party computation : a visual way , Volume 8317 of the series Lecture Notes in Computer Science pp 18-38, 23 January 2014.

10. Y. C. Hou. Visual cryptography for color images. Pattern Recognition, 36:1619–1629, 2003.

11. S. Cimato, R. Prisco, A. De Santis, Probabilistic visual cryptography schemes, Computer J. 49 (2006) 97-- 107.

12. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Visual cryptography for general access structures. Inf. Comput., 129(2):86–106, 1996.

13. Ch. Priyanka, Prof.Thaduri Venkata Ramana, T.Somashekar, " Analysis of Secret Sharing & Review on Extended Visual Cryptography Scheme", International Journal of Engineering Inventions ISSN: 2278-7461, ISBN: 2319-6491, www.ijeijournal.com Volume 1, Issue 10 (November2012) PP: 43-51 ISSN.

14. Sougata Mandal , Sankar Das, Asoke Nath, "Data Hiding and Retrieval using Visual Cryptography", International Journal of Innovative Research in Advanced Engineering (IJIRAE)Volume 1 Issue 1 (April 2014).

15. Young-Chang Hou, Zen-Yu Quan, and Hsin-Yin liao, " New Designs for Friendly Visual Cryptography Scheme", International Journal of Information and Electronics Engineering, Vol. 5, No. 1, January 2015 .