International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review of Anti Phishing Framework based on Visual Cryptography

D. N. Rewadkar[1], Asmita D. Abhyankar[2]

[1]H.O.D, Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

[2]Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

Abstract: ***With the overwhelming use of the internet in the field of E Commerce and online trade, internet attacks has been increased from last decade. Among the different internet attacks, phishing is most popular attack. Phishing is technique to steal someone's sensitive information such as passwords, account details, or credit card numbers. Fake websites are the basic source of phishing attacks .The appearance of fake website is very similar to the original one. Moreover, malicious web sites, which look very similar to original one, are used to impersonate the victim's sensitive information. Thus different ways are presented by various researchers to overcome the problem of phishing. In this paper, a novel anti phishing framework is proposed to overcome these problems***

Keywords: Phishing ,Visual Cryptography

1. Introduction

Nowadays, E commerce and online trades are become very common and there are various security threats present behind this. Among these threats, Phishing is identified most serious threat and various new ways are used by attackers. Thus, such intense security should not be tractable by implementation easiness.

Now-a-days ,most applications are only as secure as their respective system. Since the technology used has improved steadily, their detection is a difficult problem. As a result of this ,thisis nearly impossible to find out trustworthy website. The main question is how to handle applications that require a high level of security.

Particularly, Phishing attacks depend on technical deceit and social engineering practices. In most of the cases, phisher must enforce the victim to intestinally perform set of actions that will reveal the sensitive information. Moreover, email, web pages, IRC and instant messaging services are more popular as point of attack. For example, victim receives the email from abc@pqr.com, demanding for personal and bank details. This challenge of Phishing is overcome by many methods which are presented by various researchers. This paper discuss these methods along with their advantages and disadvantages.

2. Review of Different Methods

Divya James and Mintu Philip [1] used visual cryptographic technique to introduce their novel anti-phishing framework. They presented Anti-Phishing Image Captcha validation scheme based on the visual cryptography. Moreover, this method is divided into two steps: Registration phase and Login phase. In Registration phase, "key string" is used as password registration on secure website. Moreover, this "key string" is combination of alphabets and numbers and concatenated with random generated string in the server. Further, the image captcha is generated using this key string. Furthermore, in login phase, user enters username and his login share and server generates new image captcha which has to match with the one generated at time of the registration. Creation of shares is most important part of the registration phase whereas text in the image captcha is required for login phase. This method verifies the authenticity of the web sites, cross validates the image captcha and preserves intruder's attack on user account.

Moreover, Xiaoqing GU, Hongyuan WANG and Tongguang NI [2] presents an automatic approach for intelligent phishing. They used large number of legitimate and phishing webs to learn about phishing and detect phishing web sites. Moreover, they analyzes the features of Uniform Resource Locator (URL), and classified by Naïve Bayesian (NB) classifier. Furthermore, web sites are identified based on the set of words that uniquely identifies the ownership of the website. The content and structure of the websites are used to reveal the identity of the website. Moreover, Document Object Model (DOM) is used to parse the web page. Similarly, inverse document frequency technique is used to extract identity set from web page. This technique categorizes webpage features and has high detection rate because of SVM usage.

In 2000, Ren-Junn Hwang [3] proposed very popular watermark method to protect the digital image copyright ownership. This watermark method is based on visual cryptography. He proposed some characteristics of watermark method that is watermark pattern can be recognized without any information about the original message. It is very tedious to detect the pixel concerning the watermark pattern without the secret key that is secret by the owner. The watermark pattern cannot be recognized from the marked image till the retriever has the verification information and the secret key

3. Current Methodology

In the current scenario, when user wants to access his confidential information online by logging in into his account, the person enters his personal information like user

Licensed Under Creative Commons Attribution CC BY

name and password etc on the login page. But quite often, this information is captured by the attacker using phishing sites. Most of the times after this the user is directed to the original site.

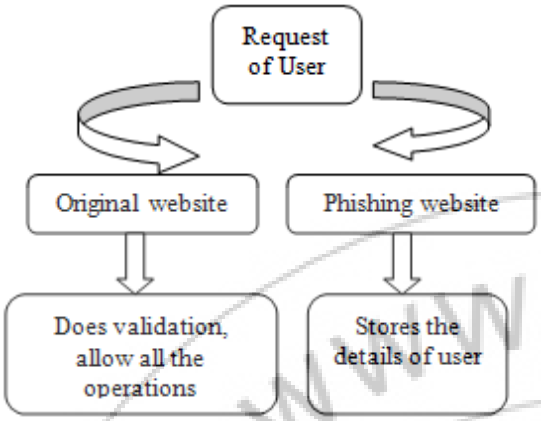

Figure 1: Current Methodology

4. Proposed Methodology

For detection of phishing detection and prevention, a new methodology is proposed to detect the fake website. This methodology is based on anti-phishing image captcha validation method using visual cryptography. It prevents user's important information from getting steeled from attacker.

Naor and Shamir[4] introduced the visual scheme which is secure way to share the images without any cryptographic computations. These cryptographic schemes are further used to derive many protocols regarding the same. Visual cryptography scheme is a technique of cryptography that takes visual information for encryption such that decryption can be performed using human visual system. In this methodology (2,2) Threshold VCS scheme is used. It is simplest threshold scheme that accepts secret message and encrypts it in two shares and reveal the secret image with the help of them.

There are two modules included :
1. Registration module
2. Login module

1. Registration Module
In this module, a string is accepted from the user at the time of registration for the secure website. This string is concatenated with the string generated at the server side and then the image captcha is generated. This image captcha is divided into two shares. One share is kept with the user and other with server. User keeps the share for the later verification of the password. One share is also kept at server side that is at any trustworthy website. Registration can be illustrated using the following figure.

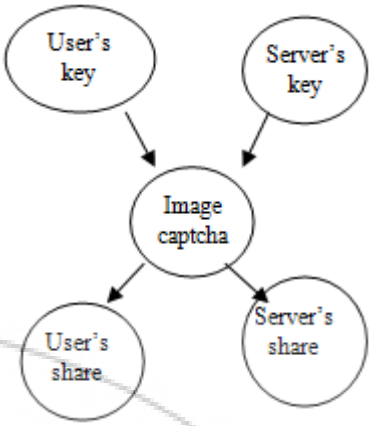

Figure 2: Registration Phase

1. Login Module
Following steps are carried out during this phase:
1)User enters username and sends the share kept with him at the time of registration to the server.
2)Server has stacked the shares of the user as well as his own
3)Now, server will display the image captcha
4)User will verify the image captcha and recognizes the object displayed as an image. Server displays the image as a well known object for example image of animals etc

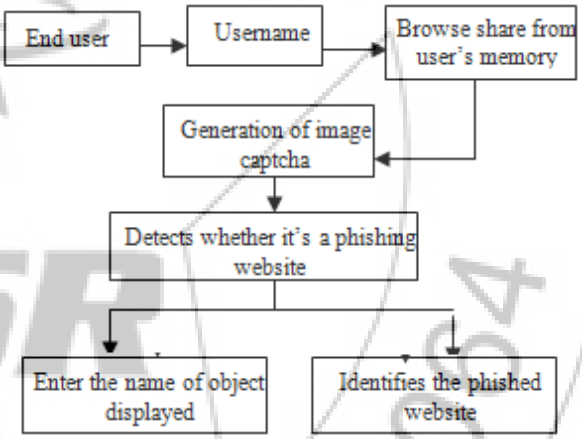

Figure 3: Login Phase

5. Conclusion

The cyber frauds are increasing day by day.The intelligent attackers are creating fake websites same as of the original/genuine websites and hence capture and store user's confidential information. By using this system it is possible to overcome above situation. The system helps to recognize the system is genuine or not and if it is not then the user's confidential information will not be revealed to the phishing website. The use of shares as a security key in this system increases the security level. This system can be used in the sectors like banking, finance and online shopping.

References

[1] Divya James,Mintu Philip,"A novel anti phishing framework based on visual cryptography,IEEE 2012
[2] Xiaoqing GU, Hongyuan WANG, Tongguang NI," An Efficient Approach to Detecting Phishing Web ✍".

Licensed Under Creative Commons Attribution CC BY

Journal of Computational Information Systems 9: 14 (2013) 5553–5560 Available at http://www.Jofcis.com

[3] Ren-Junn Hwang," A digital image copyright protection scheme based on visual cryptography",*Tamkang Journal of Science and Engineering, Vol. 3, No. 2, pp. 97-106 (2000)*

[4] Ollmann G., The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[5] M. Naor and A. Shamir, "Visual cryptography," in Proc.EUROCRYPT,1994, pp. 1–12.

[6] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.

[7] G. R. Blakley, .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[8] A. Menezes, P. Van Oorschot and S. Vanstone, .Handbook of Applied Cryptography,. CRC Press, Boca Raton, FL, 1997.

[9] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.

[10] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. IEEE Transactions, ISCAS-2004, pp.572-575.

Author Profile

Prof. D. N. Rewadkar received M.E. Computer Technology, from S.R.T.M. University, Nanded (2000).Currently he is working as the H.O.D of Computer Engineering Department in RMD SSOE, Warje, Pune. He was a Member of Board of Study committee of S.R.T Marathwada University, Nanded for Computer Science & Engineering. He has 21 years of teaching experience.

Asmita D. Abhyankar Research Scholar RMD Sinhgad School of Engineering, University of Pune. She received B.E. in Information Technology from Information Technology department of Pune Vidyarthi Griha's College of engineering and technology from University of Pune, Pune.). Currently she is pursuing M.E. in Computer Engineering from RMD Sinhgad School of Engineering, Warje, Pune, University of Pune.

Licensed Under Creative Commons Attribution CC BY