ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY

Mounika Reddy.M[1], Madhura Vani.B[2]

Student, Department of CSE, MLRIT, Hyderabad, India [1]

Asst.Professor, Department of CSE, MLRIT, Hyderabad, India [2]

ABSTRACT: Phishing is one of the attacks that became popular recently. It is an identity theft attempt in order to obtain confidential and private information of individuals or companies for monetary or other gains. In the recent part there were many reports on phishing attack in many financial domains including banking. It has become a serious threat to enterprises that deal with financial transactions. If these threats are not addressed thoroughly, people can't trust online transactions that involve due authentication through credentials. Many solutions came to solve this kind of identity theft. Recently *James and Philip* proposed a new approach based on visual cryptography to address the issue of phishing. This will automatically preserve the privacy of captcha. It achieves this by dividing the original image into two shares which are to be stored in different databases. The decryption is possible only when adversaries can provide both shared at a time. The individual shares can't reveal the original captcha. In this paper, we implement the visual cryptography using C# programming language for building an anti-phishing framework. The experimental results revealed that the proposed application is secure and can prevent phishing attacks.

Index Terms – Visual cryptography, captcha, phishing, security

I. INTRODUCTION

Due to the invention of new technologies over Internet online transactions has become a common feature in many web applications including e-commerce applications. As the transactions over Internet grow, the possibility of security threats also grows. One such threat is phishing attack which can perform identity theft. Phishing is a process of deceiving a party in order to obtain credentials and gain monetary and other gains. It is one of the security concerns. Thus it is essential to build methodology required to prevent such attacks. Phishing attacks have been recorded in the history in banking and e-commerce domains. This is because these two domains provide monetary transactions online. By stealing identity details of online users one can gain access to original web application and perform activities for which there were not authorized.

Phishing is one of the identity theft attacks that are to be handled efficiently. There were many solutions. However, recently James and Philip [1] proposed phishing attack prevention using a framework. The framework supports complete web application security with respect to phishing attacks. The proposed framework has two phases. In the first phase, a new user registers himself. While making registration the web application chooses an image then it is converted into two share images. While authentication phase, the user is asked for the two shares. Only the shares are available with original user only. Thus he phishing attacks are effectively prevented.

The rest of the paper is organized as follows. The section II provides review of literature. Section III provides proposed scheme for anti-phishing. Section IV presents prototype implementation details. Section V presents experimental results while section V concludes the paper.

II. PRIOR WORKS

Phishing attacks can be made online through a variety of means including URL, like fake web pages, Emails, and obfuscation of target web sites, VIRUS and so on. Many techniques came into existence to prevent phishing attacks. One such method is automated challenge response method [2].Afterwards DNS-based approach came to combat anti-phishing [3]. This technique makes use of blacklist, white list concepts. In [4] Spoof Guard was proposed to prevent phishing attacks. Later on CANTINA [5] came into existence which is detecting web sites based on content similarity. Page visual similarity techniques were used in [6], [7] for detecting phishing attacks. URL similarity assessment technique is used by Kang and Lee [8]. An authentication scheme known as Phish-Secure came into existence [9] which is basically a counter attack phishing.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

However, all these drawbacks have a common thread that blacklist-based solution has certain limitations; Heuristic based Anti-phishing has high probability of false positives; it is time consuming to use similarity based approaches. In [10] anti phishing is achieved by data-eXploration which is a form of retrospection. In [11] a new approach is proposed which needs two types of passwords to access web applications.

Later in [12] Modeling Intelligent Phishing Detection System was developed based on data of e-banking. This is intelligent and used in banking domain. Visual content based anti-phishing technique came in [13] proposed by Zhang et al. It is based on the cues.

Finally in [1] a visual cryptography based anti-phishing mechanism was proposed. It uses a graphical captcha that generates two shares. The shares are used as part of authentication. Only genuine users can provide these shares.

III. PROPOSED METHOD FOR ANTI-PHISHING

The proposed methodology has two phases. They are known as registration and authentication. In the registration phase, user enters a key, server enters a key and them captcha image is presented. The image is divided into two shares in such a way that the shares when stacked together should restore the original captcha.

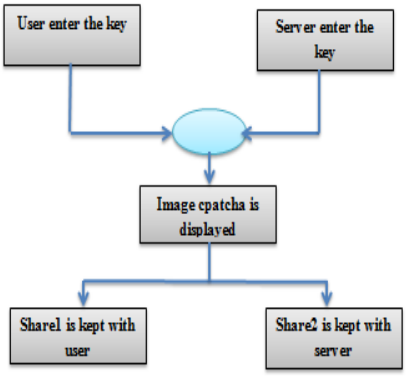

Fig. 1 – Mechanism in registration phase

As can be seen in fig. 1, the operations in registration phase are presented. In the login phase actual authentication takes place. The authentication process is built in such a way that it can detect any kind of phishing attack. In fact it can prevent fishing attack.

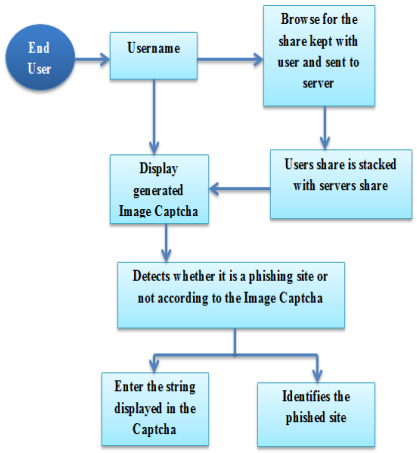

Fig. 2 – Login Phase mechanisms for anti-phishing

As can be seen in fig. 2, the end user given credentials and then chooses the share of the captcha given to him at the time of registration. Then the server sends its corresponding share. By stacking these two shares, the original captcha is established. The original captcha can find whether the user is really genuine user or a phishing attack is carried out. The login mechanism can identify phishing activity and prevent it efficient with 100% true positives.

IV. PROTOTYPE IMPLEMENTATION

The prototype application is built to demonstrate the proof of concept. The environment used to build the application includes a PC with 2 GB RAM, Core 2 dual processor running Windows operating system. The platform used to develop the application Microsoft .NET 4.0 and the development tool is Visual Studio 2010.

V. EXPERIMENTAL RESULTS

The experiments are made using various captcha images. The proposed technique used to detect phishing attack is successful whenever the test is carried out. The experimental results are as presented in table 1.

NUMBER OF EXPERIMENTS	100
FALSE POSITIVE PERCENTAGE	0
TRUE POSITIVE PERCENTAGE	100

Table 1 – Experimental results

As can be seen in table 1, it is evident that the application demonstrates 100% true positives. Therefore it can be concluded that phishing attack is not possible in the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

application where this technique is practically applied. The results are reflected in fig. 3.

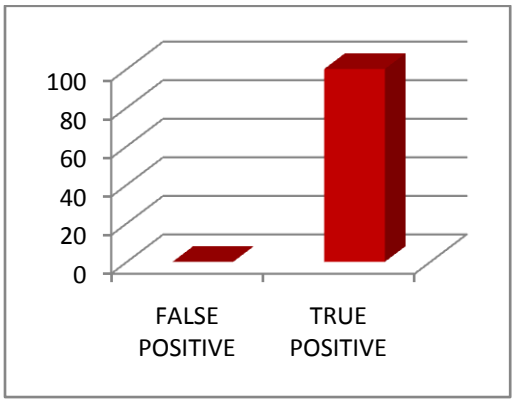

Fig. 3 – Visualization of Experimental Results

As can be seen in fig. 3, the average results of 100 experiments are presented. Zero false positives and 100% true positives are presented. The horizontal axis represents the category of results while the vertical axis represents the % of success of the experiments. The overall results reveal that the proposed mechanism for detecting and preventing phishing attack is very effective and can be used in the real world applications.

VI. CONCLUSION

Phishing attacks are well known attacks as they can obtain sensitive information from online users. Attackers use such information for monetary benefits. In this paper we implement a new anti-phishing methodology proposed in [1]. It is nothing but visual cryptography in which image captcha is used to prevent identity theft. When a new user is registered a captcha is associated with the user profile. The captcha image is converted into two shares which are to be kept secret. Only the original user can provide the shares. When both the shares are provided by the user, then only the authentication process gets completed. Thus the proposed system provides complete security to the web site from phishing attacks. We built a prototype web application that demonstrates the proof of concept. The empirical results reveal that the proposed anti-phishing scheme is effective and can be used in real time applications.

REFERENCES

[1] Divya James and Mintu Philip," A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY "International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[2] Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method"', in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.

[3] Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010

[4] Nourian, A.; Ishtiaq, S.; Maheswaran, M.;" CASTLE: A social framework for collaborative antiphishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing:Networking, Applications and Worksharing, 2009.

[5] Sid Stamm, Zulfikar Ramzan, "Drive-By Pharming", v4861 LNCS,p495-506, 2007, Information and Communications Security - 9th International Conference, ICICS 2007, Proceedings.

[6] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3, n 4, p301-311, October/December 2006

[7] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Antiphishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.

[8] JungMin Kang, DoHoon Lee, "Advanced White List Approach for Preventing Access to Phishing Sites", 2007 International Conference onConvergence Information Technology, ICCIT 2007, p 491-496, 2007

[9] Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.

[10] 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.

[11] Qingxiang Feng.; Kuo-Kun Tseng.; Jeng-Shyang Pan.; Peng Cheng and Charles Chen.; "New Antiphishing Method with Two Types of Passwords in OpenID System", in Proceedings of IEEE Fifth International Conference on Genetic and Evolutionary Computing,2011

[12] Maher Aburrous .; M. A. Hossain.; Keshav Dahal.; "Modelling Intelligent Phishing Detection System for e-Banking using Fuzzy Data Mining", in Proceedings of IEEE Conference on CyberWorlds,2009.

[13] Haijun Zhang , Gang Liu, and Tommy W. S. Chow, "Textual and Visual Content-Based Anti-Phishing:A Bayesian Approach," *IEEE Trans. Neural Netw.*, vol. 22, no. 10, pp. 1532–1546, Oct. 2011.