Image Captcha Based Authentication using Visual Cryptography

Mohit Yadav[1], Ashwita Ram[2], Aaishwarya Bhoir[3], Shirish Sabnis[4]

[1 2 3]*Student, Information Technology, Rajiv Gandhi Institute of Technology, Maharashtra, India*
[4] *Faculty, Information Technology, Rajiv Gandhi Institute of Technology, Maharashtra, India*

ABSTRACT

Phishing is an attempt by an individual or a group to steal personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. In this project we have proposed a new approach named as "A Novel Antiphishing framework based on visual cryptography" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (VC) is used. The use of visual cryptography is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both(client,server) are simultaneously available; and the another phase is during the registration the user have to select any random images which will be useful for authentication of user when he tries to login. the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. .

Keyword: *Antiphishing, Captcha, Visual Cryptography, Shares*

1. Introduction

Phishing is an attempt by an individual or a group to get confidential information such as passwords and credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Phishing is an act of attempting to acquire sensitive information of a person by masquerading as a trust worthy entity in electronic transaction. Phishing is typically carried out by e-mail spoofing or instant messaging. Phishing e-mails contain links to websites infected with malware. Phishing is generally carried out through e-mail spoofing and by mimicking the web ages of original websites which look exactly the original ones. Here, attacker sends a mail to the person whose details he wants to track. In the mail attacker hides his true identity and generally he sends a link which appears similar to the genuine website like bank website etc.., here, attacker adds some message to mislead the user. Innocent users think it is true and they login to the site providing their credentials and thus falling prey for Phishing attack. So here introduces a new and secure method which can be used to prevent phishing attacks which is named as "An Anti-phishing framework with interactive captcha validation scheme using visual cryptography". In this method, we provide a provision to the user to check whether the website he is willing to visit is a genuine website or a phishing website. So, by knowing these he can securely perform his further proceedings or transactions. Here, we used the concept of an improved visual cryptography. Visual Cryptography (VC) is used here to divide the image captcha into shares and in order to reveal the original image captcha appropriate number of shares should be combined.

2. LITERATURE REVIEW

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 antiphishing [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.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-explorations 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.

3. PROPOSED METHODOLOGY

In order to prevent phishing attacks, we are proposing a new methodology which is helpful to detect the phishing website. Our methodology helps the user to protect their password and other confidential and sensitive information from the phishing websites.

In our proposed methodology, we are using here two phases for authentication of a genuine user and also prevent user from phishing attack.

3.1. Registration Phase

In Registration phase, user 1st visits the site manually. The web administrator provides a registration form to the user. User will fill all the required details. At the time of registration the user have to select random images, which will be useful for the user during the time of login .at the same time the user have to enter the captcha value. The captcha image will be divided into 2 parts. One part of image will be stored in server another part of image will be stored in client machine

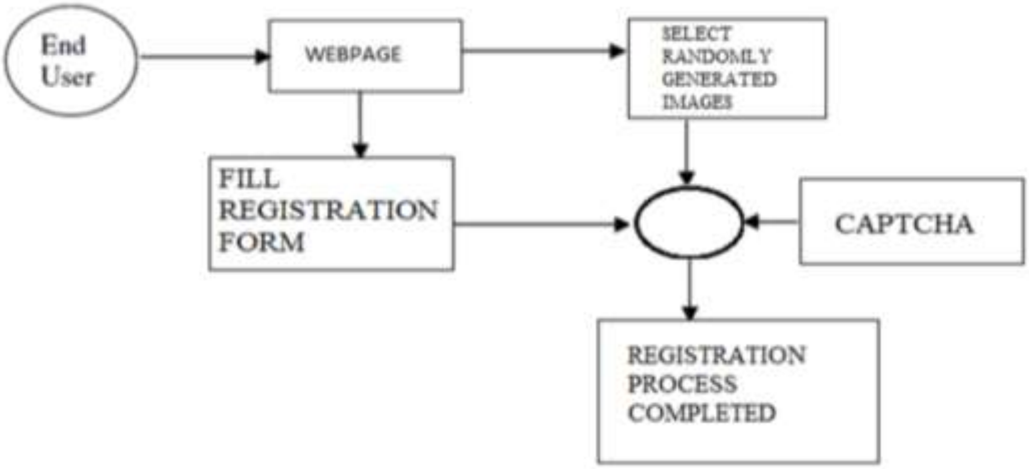

End User
WEBPAGE
SELECT RANDOMLY GENERATED IMAGES
FILL REGISTRATION FORM
CAPTCHA
REGISTRATION PROCESS COMPLETED

Fig -1: Registration Phase

3.2. Login Phase

In Login Phase, First the user will access the website. The user will enter his login id and password ,after that the user have to select the images which he has chosen during the time of registration, and after that the user have to upload the captcha image. If both the phases matches then only the user can login into the website

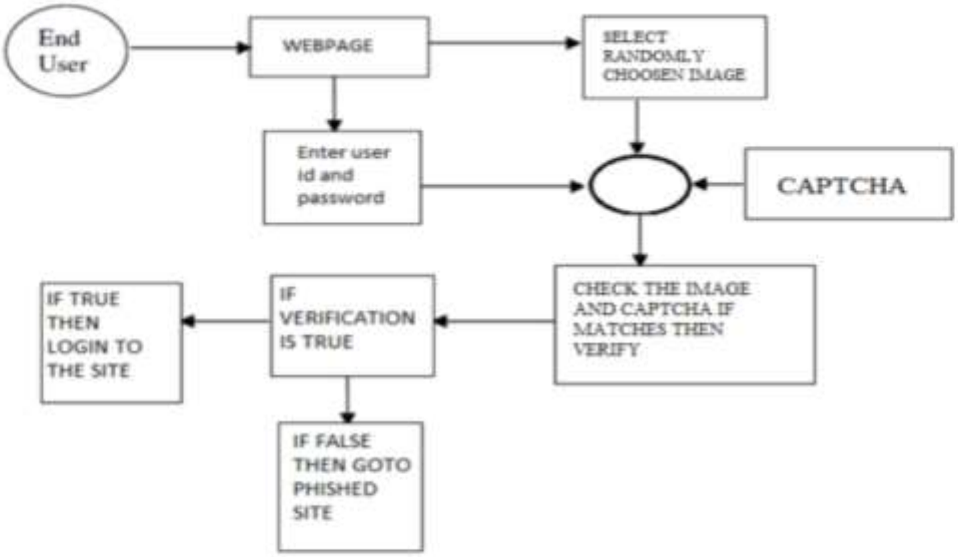
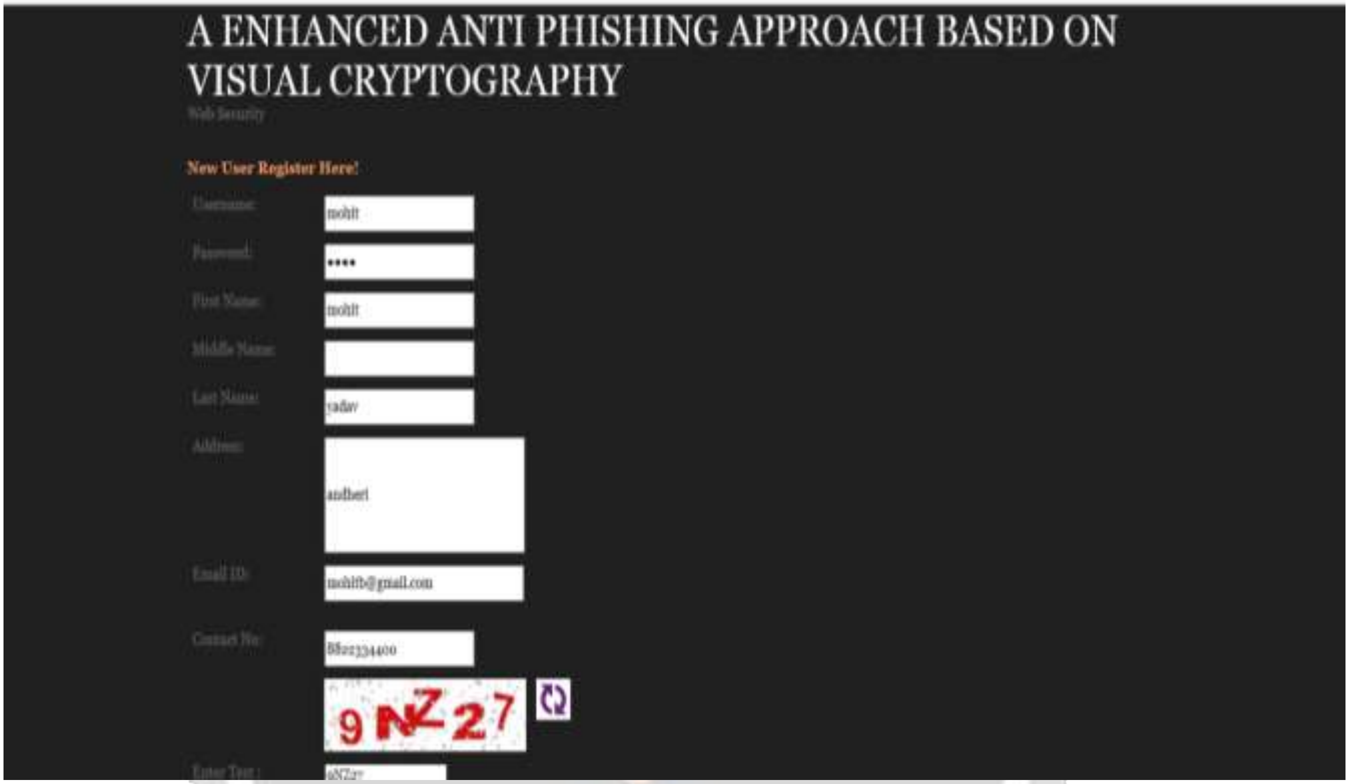

End User
WEBPAGE
SELECT RANDOMLY CHOOSEN IMAGE
Enter user id and password
CAPTCHA
CHECK THE IMAGE AND CAPTCHA IF MATCHES THEN VERIFY
IF VERIFICATION IS TRUE
IF TRUE THEN LOGIN TO THE SITE
IF FALSE THEN GOTO PHISHED SITE

Fig -2: Login Phase

4. IMPLEMENTATION

The project is been implemented using Microsoft visual studio10, sql server12.The programming Languages used are c#, asp.net. The user 1st visits the website, if the user is new user he registers first by entering his information.

All his information is stored on server database. During registration the user is allowed to enter the captcha, after entering the captcha the user is given his share of equivalent image captcha. So during time of login the users only need to enter his valid id and password and browse his image share that was provided to user during registration. If the user enters the correct id and password, and also if he presents the correct share of his image then he is authorized to access the site.



A ENHANCED ANTI PHISHING APPROACH BASED ON VISUAL CRYPTOGRAPHY

Web Security

New User Register Here!

Username:	mohit
Password:	••••
First Name:	mohit
Middle Name:	
Last Name:	yadav
Address:	andheri
Email ID:	mohitb@gmail.com
Contact No:	8802334400
Enter Text :	9NZ27

5. ACKNOWLEDGEMENT

I sincerely thanks to all authors in reference section. All papers in the reference section are very useful for my proposal. Their concepts, algorithms and techniques are very useful for my Project

6. 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.

7. 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: Largescale 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.