International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Prevention of Phishing Threats using Visual Cryptography and One Time Password (OTP)

Sneha M. Shelke[1], Prachi A. Joshi[2]

[1, 2]Department of Computer Science and Engineering, Deogiri Institute of Engineering and Management Studies, Aurangabad (MS), India

Abstract: ***Internet is today's common need and it's being used for many purposes such as Email, business, shopping, e-commerce, social networking, financial transaction etc. With the increasing dependence on internet, the possibility of cheating/threats has been increasing day by day. One such threat is phishing attack which can perform identity theft. Phishing is the criminal and fraudulent act of attempting to acquire sensitive information such as username, passwords, account IDs, and credit card information etc by masquerading as a trustworthy entity in an electronic communication. The information thus acquired may be re-sold or used to cause financial losses. In the Internet, phishing can reach the user in several ways, e.g., through a web browser pop-up, instant messaging or email. Recently a number of phishing attacks are increasing more and more. Hence there is a need for efficient mechanism for the prevention of phishing. In this paper, Cryptography and authenticating along with dynamic OTP has been proposed to recognize the whether the site is safe or unsafe to carry out transaction.***

Keywords: Phishing, Visual cryptography share, OTP

1. Introduction

Now a days, Internet is common need and provides the backbone for modern living enabling ordinary people to shop, socialize, financial transaction, access all kinds of information anytime from anywhere and be entertained all thorough their own computers. As people's reliance on the Internet grows, so the possibility of hacking and other security breaches increases regularly [1]. One such threat is phishing attack which can perform identity theft [1-4].

In the past few years, phishing has become one of the major issues and the number of phishing attacks is increasing more and more [2]. Lot of users becomes victim to these attacks. Phishing websites are a replica of genuine websites. Phishing website has visual similarity and website pages look exactly like real web pages. Only specialists can identify these types of phishing websites immediately. But all the web users are not specializing in the computer engineering and hence they become victim by providing their personal details to the phishing artist. Phishing is continuously evolving since it is easy to copy an entire website using the HTML source code. By making slight changes in the source code, it is possible to direct the victim to the phishing website. Phisher uses a lot of techniques to lure the unsuspected web user. They send generic greetings to the customers to check their account immediately. They also send threat messages indicating to update their account immediately; otherwise their account will be cancelled. Thus an efficient mechanism is required to identify the phishing websites from the legitimate websites in order to save credential data [5].

In the Internet, phishing can reach the user in several ways, e.g., through a web browser pop-up, instant messaging or e-mail. Usually, the victim is persuaded to perform a mouse click to download and install malicious code or access a fraudulent web site without being aware of it [6].

In email-born phishing attacks, first the attacker creates a faked web site which appears genuine website. Using some tools hackers send lots of spoofed emails to target users in the name of legitimate companies and organizations, trying to convince victims to visit their websites. Phishing emails are nearly identical to the normal emails; it is quite difficult for the average users to distinguish phishing emails from non-phishing once. Moreover, phishing tactics have become more and more complicated and the phishers continually change their ways of perpetrating phishing attacks to defeat the anti-phishing techniques. The email generally contain a link which ask the recipient to supply confidential information, such as bank account details, passwords and these details are then used by the owners of the website to conduct fraud. Once the user's input their information, the phishers collects that information and used to access the account by logging into your account. In some cases, the phishers implant malicious software that controls a computer so that it can participate in future phishing scams [6-8].

In email-born phishing attacks, phisher sends emails that mislead victims into revealing credential information such as account numbers, passwords, or other personal information to the phisher. For example, fisher send the fake e-mail message to the bank user's, as if the database of the bank has been crashed due to some technical reasons, so they request you for updation of the personal information. As most phishing emails are nearly identical to the normal emails, it is quite difficult for the average users to distinguish phishing emails from non-phishing once. Moreover, phishing tactics have become more and more complicated and the phishers continually change their ways of perpetrating phishing attacks to defeat the anti-phishing techniques.

2. Visual Cryptography

Cryptography is an essential tool to protect the data that transmits between users by encrypting the data so that only intended users with appropriate keys can decrypt the data. It uses human visual system hence need not required a

computer. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available. Cryptography is the most commonly used mechanism in protecting data. A survey conducted by Computer Security Institute in 2007 revealed that 71% of companies utilized encryption for their data in transit [3, 7].

Visual cryptography is first proposed by Nior and Shamir to protect secrets [13]. They analyzed that the visual cryptography has two important features. The first feature is its perfect secrecy and the second is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some authorized set of shares. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available. The simple decryption method is the reason that attracts many researchers to make further detailed inquiries in this research area.

Many related methods concerning the theory and the applications of visual cryptography have been proposed by researcher. An extended visual cryptography scheme, colored visual cryptography scheme has been studied by researchers. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [9, 14-16]. Text Graphics Character CAPTCHA [12], Color images based visual cryptography [17] have been studied.

Recently, more and more applications of visual cryptography, such as authentication, human identification, copyright protection, watermarking, mobile ticket validation, visual signature checking etc. are introduced [18, 19]. The most of the constructions of visual cryptography schemes are realized using two n × m matrices, S0 and S1, called basis matrices. The general method for the construction of basis matrices is discussed below.

A. Various Visual Cryptography Schemes (VCS)

The general construction of various visual cryptography schemes is as follows

1) (2, 2) Threshold visual cryptography scheme: In this scheme, a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.
2) (2, n) Threshold visual cryptography scheme: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.
3) (n, n) Threshold visual cryptography scheme: This scheme encrypts the secret image to n shares such that when all n of the shares are combined the secret image is revealed. The user will be prompted for n, the number of participants.
4) (k, n) Threshold visual cryptography scheme: This scheme says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image. If the number of shares stacked is less than k, the original image is not revealed.

Let us consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S1 and S2, consisting of exactly two pixels for each pixel in the secret image as shown in Table 1. If the pixel in S is white, the dealer randomly chooses one row from the first two rows of Table 1. Similarly, if the pixel in S is black, the dealer randomly chooses one row from the last two rows of Table 1.

Table 1: Pixel pattern for (2,2) VCS with 2-subpixel layout

Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
	0			
	0			
	1			
	1			

To analyze the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table 1 for the shares S1 and S2. The pixel selection is random so that the shares S1 and S2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. This method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared subpixels. If the superimposition results in two black subpixels, the original pixel was black; if the superimposition creates one black and one white sub-pixel, it indicates that the original pixel was white. In visual cryptography, the white pixel is representing by 0 and the black pixel by 1. Implementation of (2,2) and (2,3) VCS is given below.

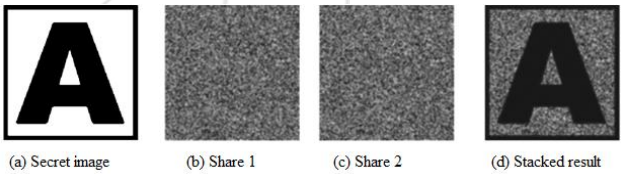

Figure 1: Implementation of a (2, 2) VCS

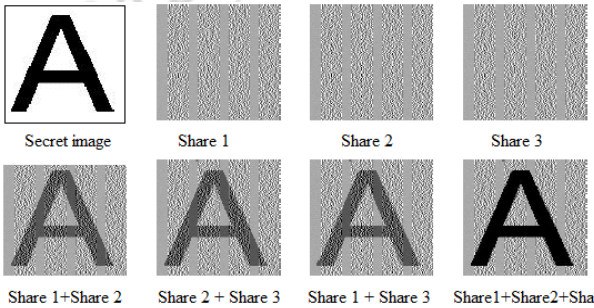

Figure 2: Implementation of a (2, 3) VCS

3. One Time Password (OTP)

One-time passwords are passwords that are used once and only valid for one login session or transaction. Banks, governments and other security based industries deploying OTP system where user may have many passwords and use each password only once. OTPs can avoid a number of shortcomings that are associated with traditional passwords which are valid for many transactions as users are reluctant to

voluntarily change passwords frequently. Since OTPs are only valid for single use, an attacker has a smaller window of time to gain access to resources guarded by such a password because any previously stolen passwords will likely have become invalid[22].

There are mainly two types of password
- Static password
- Dynamic Password

Static password is the traditional password which is usually changed only when it is necessary. It is changed when the user has to reset the password, i.e., either the user has forgotten the password or the password has expired. Static passwords are highly susceptible to cracking, because passwords used will get cached on the hard drives. Unlike a static password, dynamic password is a password which changes every time the user logs in. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker. This reduces the vulnerability of the hacker sniffing network traffic, retrieving a password, and to successfully authenticate as an authorized user. This password is used only for that session and when the user logins next time, another password is generated dynamically. Image based authentication is included to provide additional security integrated with OTP. With IBA, when the user performs first time registration on a website, he makes a choice of several secret categories of images that are easy to remember, such as pictures of natural scenery, automobiles. Every time the user logs in, a grid of randomly generated images is presented to the user. The user identifies images that were previously selected. One-time access code is generated by the selected images, making the authentication process more secure than using only a static text password. It's significantly easier and advantageous for the user because he has to remember only a few categories to recognize the selected images.

Various approaches for the generation of OTPs are listed below:
- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time).
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order)

Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter [23].

4. Current Methodology

The figure 3 represents the current scenario, when the end user wants to access his/her confidential information or want to do financial transaction online by logging into his/her bank account or secure mail account, the user enters information like username, password, credit card number etc. on the login page. This information can be captured by attackers using fake site. In such case, phishing website can collect the login information the user enters and redirect and such information may be re-sold or used to cause financial losses.

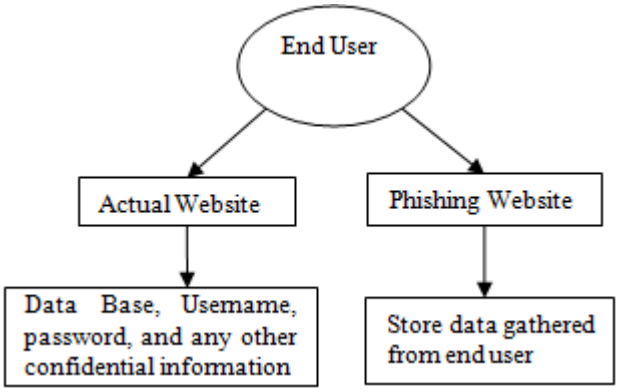

Figure 3: Current scenario

5. Proposed Methodology

The figure 4 shows proposed methodology to detect phishing attacks. This methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography and OTP. Combination of captcha and OTP validation provides secure authentication. It prevents password and other confidential information from the phishing websites. The proposed approach can be divided into two phases:

Phase I: Registration

During registration phase, end user has to provide user name, email ID and mobile number for the secure website. The user string can be a combination of alphabets and numbers to provide more secure environment. Based on the information provided by the user, OTP and image captcha is randomly generated by server. The image captcha is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image along with OTP are sent to the user for later verification during login phase. The image and OTP is also stored in the actual database of any confidential website as confidential data. Because an image is used as the password at first tier later. Registration process with sequence of encryption is depicted in figure 4.

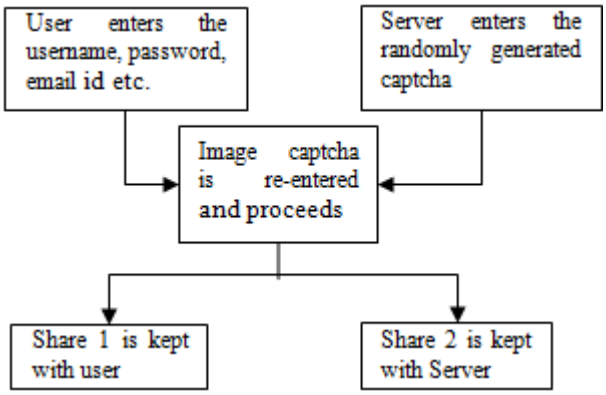

Figure 4: Registration Phase

Phase II: Login Phase

In the login phase, first user has to enter user name. Then user is asked to enter half share image which is kept with him/her. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to generate the image captcha. The generated image will be displayed to user and user should compare the generated image with the original image. At this moment the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. If displayed images and captcha are same, user can complete the login process and user can generate the new OTP immediately when the login is successful otherwise user have to verify the website is genuine or fake. This phase is shown in figure 5.

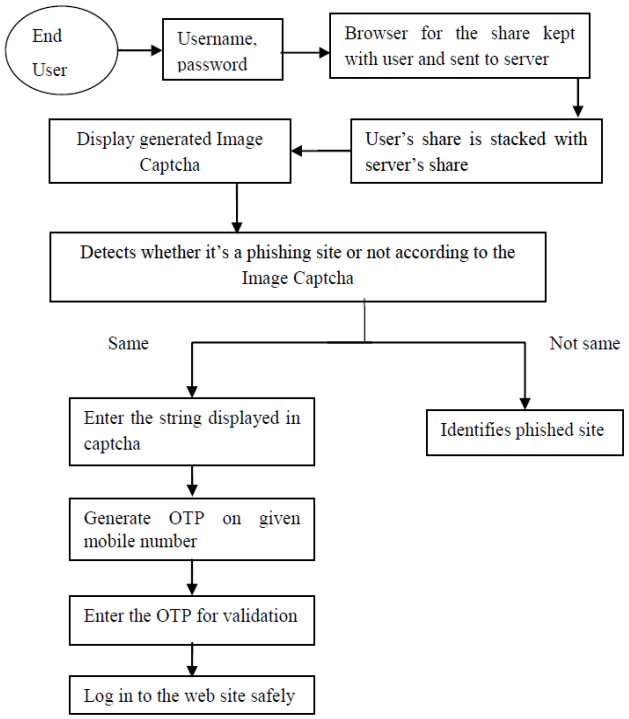

Figure 5: Login Phase

6. Implementation and Analysis

The proposed methodology is implemented using dot net. The creation and stacking of shares have been developed using (2,2) and (2,4) visual cryptography schemes. Analysis of images is carried out using MATLAB. Comparative analysis is presented in Table 2.

Table 2: Comparative analysis

Comparative parameters	(2,2) VCS	(2,4) VCS
Image quality	High	Low
Computational complexity	Less	More
Pixel expansion	Yes	Minimal expansion
Number of share	2	4
Number of white pixel in stack image	21755	34269
Number of black pixel in stack image	24567	12053
Type of secrete	Random	Random
Contrast	Better	Optimal
Correlation coefficient(Original captcha and reconstructed captcha)	0.9565	0.1500

7. Conclusion

Nowadays phishing has become one of the major issues and the number of phishing attacks is increasing more and more. Personal information is acquired in an electronic communication to cause financial losses. Lot of users becomes victim to these attacks. Hence s strong anti fishing mechanism is required. The proposed method preserves secret information of users. In this paper, anti fishing solution based on visual cryptography has been presented. Using proposed method, end user can easily identify the website is genuine or fake based on validation of image captcha. Additional security is provided by using OTP. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is useful for financial web portal, banking portal and online shopping market to prevent the attacks of phishing websites.

References

[1] Liang H., & Xue Y., "Understanding security behaviors in personal computer usage: A threat avoidance perspective", Association for Information Systems, 11(7), pp. 394–413, 2010.
[2] Nalin Asanka Gamagedara Arachchilage, Steve Love, Security awareness of computer users: A phishing threat avoidance Perspective, Computers in Human Behavior (38), pp. 304–312, 2014.
[3] Yuancheng Lia et al., "A semi-supervised learning approach for detection of phishing web pages", Optik, (124), pp. 6027– 6033, 2013.
[4] Anti-Phishing Working Group (APWG), Phishing activity trends report for the month of June, 2007 http://www.antiphishing.org/
[5] Isredza Rahmi A. Hamid, Jemal H. Abawajy, "An approach for profiling phishing activities" computers & security 45 (2014) pp. 27 -41
[6] Cleber K. Olivo, Altair O. Santin, Luiz S. Oliveiraba "Obtaining the threat model for e-mail phishing", Applied Soft Computing 13 (2013) 4841–4848Julian Jang- Jaccard ,
[7] Surya Nepal, "A survey of emerging threats in cyber security" Journal of Computer and System Sciences 80 (2014), pp. 973–993
[8] Won Kim, Ok-Ran Jeong, ChulyunKim, Jungmin So The dark side of the Internet: Attacks, costs and responses, Information Systems, 36 (2011), pp. 675–705
[9] Carlo Blundo, Stelvio Cimato, Alfredo De Santis, Visual cryptography schemes with optimal pixel expansion, Theoretical Computer Science, 369 (2006), pp. 169 - 182
[10] Santhana Lakshmi V, Vijaya MS, Efficient prediction of phishing websites using supervised learning algorithms, Procedia Engineering 30 (2012), pp. 798 - 805
[11] 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 Intelligence, 2010.

[12] Divya James, Mintu Philip, A novel anti phishing framework based on visual cryptography, International Journal of Distributed and Parallel System, Vol.3, No.1, 2012, pp. 207-217
[13] M. Naor and A. Shamir, Visual Cryptography, Advances in Cryptology-Eurocrypt'94, LNCS 950, pp. 1-12, 1995.
[14] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes, in Journal on Cryptography, vol. 12, 1999, pp. 261-289.
[15] P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with speci_ed Whiteness Levels of Reconstructed Pixels,. Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.
[16] E. R. Verheul and H. C. A. Van Tilborg, .Constructions and Properties of k out of n Visual Secret Sharing Schemes,. Designs, Codes, Cryptography, vol. 11, no. 2, 1997, pp. 179-196.
[17] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 584–591.
[18] Chen-Chang Wang, Shen-Chuan Tai and Chong-Shou Yu, Repeating Image Watermarking Technique by the Visual Cryptography, IEICE Trans. Fundamentals, E83–A(8) : 1589– 1598, 2000.
[19] Yan,W.Q., Jin, D., Kankanhalli, M.S.: Visual cryptography for print and scan applications.In: Proceedings of International Symposium on Circuits and Systems, Vancouver, Canada, pp. 572–575, 2004.
[20] http://www.phishing.org
[21] https://www.us-cert.gov/report-phishing
[22] Himika Parmar, Nancy Nainan and Sumaiya Thaseen (2012), Generation of Secure One-Time Password Based On Image Authentication, CS & IT-CSCP, 07, 195-206.
[23] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.