THE EFFECTIVENESS OF AN INVISIBLE SECURITY IMAGE IN INTERNET BANKING

L. Karthika[1], V. Perumal[2]

Abstract **– Nowadays online transactions are becoming very common. Most of the people using online websites for their personal needs on e-shopping, e-tickets etc. Mean while the hackers are also very much interested to observe our credential details. These kind of attack is named as a phishing attach. In these situation a simple username and password authentication is not so sufficient. Today, most applications are only as secure as their underlying system. Since an implementation methodology of middleware has improvised linearly, their detection becoming very challenging task. To overcome these kind of attack a web based methodology has to be used. In past there are many ideas are implemented for anti-phishing, but it is not more efficient. One of the visual cryptographic technique is proposed to avoid the phishing websites. Image based authorization provide more secure authentication in an online banking website.**

Keywords - Phishing, Random key generation., Security image share, Visual Cryptography.

I. INTRODUCTION

In an exiting online bank website contain user ID and password as an authentication, their is a chance to mimic these website. User who is not aware of phishing site may reveal their credential detail in phishing site. Online study of 482 users that attempts to clarify the extent to which users notice and react to the absence of security images.[6]. In an eavesdropping attack, the hacker may configures that respective network interface in the promiscuous mode. Man-in-the-middle (MITM) attack to intercept communication between a client and a server.[4] About 80% of phishing and pharming attacks are directed at the payment and financial service.[9]. As per Figure 1, Phishing attack is classified.

Manuscript received Mar, 2016.

L.Karthika*, PG Scholar, Department of computer science and engineering, Saveetha Engineering College, Chennai, India.*

V.Perumal*, M.E.,(PhD), Associate Professor, Department of computer science and engineering, Saveetha Engineering College, Chennai, India.*

1. *Types of Phishing Attack.*

A. *Deceptive Phishing.*

Deceptive phishing is an attempt to deceptively capture end users personal and other secured information through an internet for their future financial benefit. An information are observed through a phishing website, which is a mimic of an original online banking website.

B. *Malware-based Phishing*

Malware-based phishing is a form of intrusion on an information security. Malware can be spread as an email attachment, as a downloadable file from a website or a spam message. A particular issue for small and medium businesses who are not always able to keep their software applications up to date.

C. *Key loggers and Screen loggers*

Key loggers and screen loggers is an attack a malware which keep tracking a keyboard input and a touch screen input. It capture and send the relevant information to the hacker through Internet. A tracking software is embed into user browser as small utility programs known as helper of an objects. It runs automatically when the browser is open as well as into system files as device drivers or screen monitors.

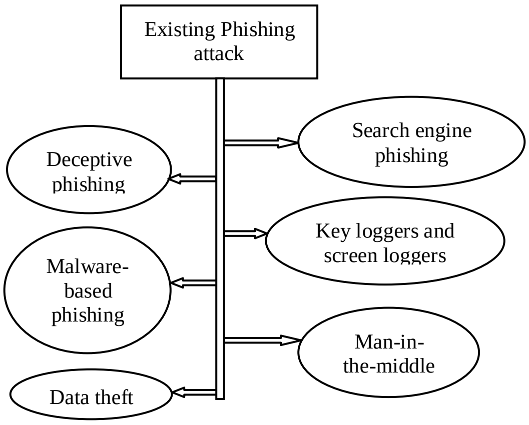


Fig. 1 Existing Phishing Attack

D. Man-in-the-middle Phishing

Man-in-the-middle is a type of intermediate between an end user and the legitimate site. The hacker wont interrupt the activity of an user, they capture their credential details. Later they can make use of that information or credentials collected when the user is not available on the system.

E. Search Engine Phishing

Search engine phishing occurs when phisher create a fake website which is a mimic of original website with an attractive advertisements. Users saw the websites in the browser, while searching for an information which is required. User may be fooled by entering their information in fake site. For example, scammers have set up fake banking sites with lower interest loan and lower credit rate offers.

F. Data theft

Data theft is an activity of stealing a computerized information without the knowledge of authorized user. Data may be stolen from desktop, laptop, hand held devices etc. As the technology develops the rate of data theft also getting increase.

II. VISUAL CRYPTOGRAPHY SCHEME

2. *Visual Cryptography*

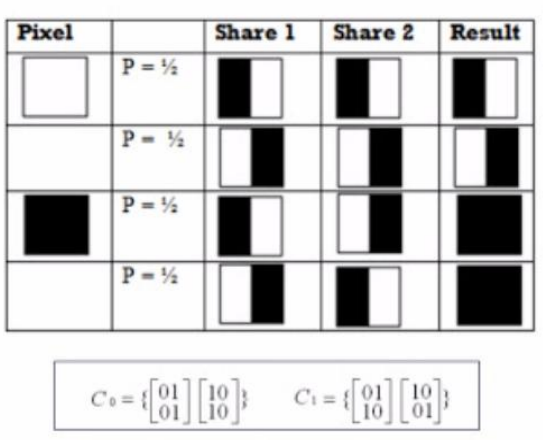
Visual cryptography is a technique, which converts the media type of data like image, video into a cipher input (encrypt). Also reconvert the cipher input as an original data in the decryption.

A. Visual Cryptography Scheme

VCS is a one of the cryptography technique which allows a visual information to be encrypted into cipher information and the decryption is a reverse process that done based on human knowledge. We can achieve this by one of the following access structure schemes.

- (2,2) Threshold VCS scheme – In this threshold scheme that takes a secret message and encrypt into two different shares, which reveal that secret image when they are overlaid.
- (n, n) Threshold VCS scheme – In this threshold scheme image will be encrypted into n shares, which reveal that secret image when all of those n shares are grouped together.
- (k, n) Threshold VCS scheme – In this threshold scheme secret image will be encrypted into n shares, which reveal that secret image when atleast any k shares are group together.

From the above three method, the first method (2,2) threshold scheme will be suitable for the proposed methodology. Since, online banking is a more confidential sector between an end user and the bank. Fig. 2. Represents the way of share creation using the black and white pixels.



$$C_0 = \{\begin{bmatrix}01\\01\end{bmatrix}\begin{bmatrix}10\\10\end{bmatrix}\} \qquad C_1 = \{\begin{bmatrix}01\\10\end{bmatrix}\begin{bmatrix}10\\01\end{bmatrix}\}$$

Fig. 2. VCS (2,2) Threshold Scheme

In Fig .2. It denotes, the shares of a white pixel and a black pixel. Each pixel in an image is randomly determined as an black and white pixels. If pixel is white then separate it as black and white pixel. Else if it is a black pixel again it will separated as two black pixels using a independent random choices.

B. Meaningful Shares in Visual Secret Sharing Scheme

The VCS(k,n) visual secret sharing scheme (VSSS) propose a binary secret image, is encrypted into n shares which is named as a transparency. Each share contain bth the black and white pixels, which may be in the form of noise and also has a larger size image than that of the secret image. The binary secret image can be decrypted by using the visual system through superimposing any VCS(k,n) transparency that is without performing any cryptography computation. To overcome these kind of problem, this system takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparency and stacking them together. While the previous researches basically handle only binary images, but this establishes the extended visual cryptography scheme suitable for natural images. Advantage is to extend the schemes and encrypt n shares as meaningful. Disadvantage of this technique is in practice, meaningless shares, however, might invite the adversary attention and to manage numerous increasing transparency belonging to different secrets is also a problem.

C. Random Pattern algorithm

Random pattern algorithms to encrypt a binary secret image. The input of the algorithm is a w × h image, denoted by A, and the outputs are two images R1 and R2. One of their algorithms is shown as below. Based on the above algorithm, this work proposes a new algorithm, process one gray-level secret image, denoted by B, and generates two gray-level encrypted images, denoted by

G1 and G2, that all pixels are classified into more than two colors.

```
Generate a w × h random grid R1
                                          // $\Im(R1) = ½$
  for( i = 0 ; i < w ; i ++ )
  for( j = 0 ; j < h ; j ++ )
     if( A[i][j] == 0 )
      {
        R2 [i][j] = R1 [i][j] ;
      }
        Else
     {
        R2 [i][j] = R1 [i][j] ;
      }
        output ( R1 , R2 )
```

When user overlaps those two encrypted images G1 and G2, the hidden secrets of the gray-level image B can be shown. According to the range of RGB value in gray-level, two methods below are concluded to encrypt every pixel on the gray-level secret image.

III. Proposed Architecture`

First the process starts from registration phase, Users are requested to fill their personal detail which includes username and password along with a maximum of eight digit secret code. Secret code can be both character and numbers. Username should be unique. All the fields are mandatory so user personal details are given at the time of registration.

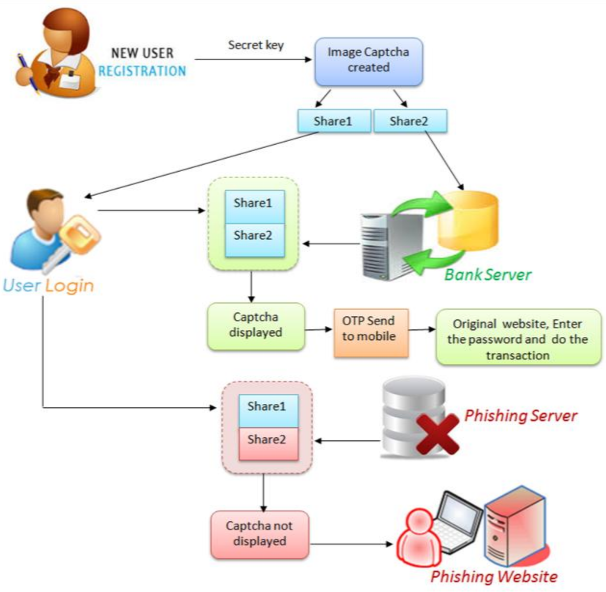


Fig. 3. Proposed Architecture

User details are stored securely in a bank database. Email notification will send to that corresponding mail ID. As stated in the Fig. 3. A security image is generated based on user and random key. The image is separated as a share using VCS(2,2). Share1 is given to user and Share2 stored in bank server. At the time of authentication the both shares will be revealed and security image caption is displayed. Then one time password will be send to the given corresponding contact number and finally transaction is done.

B. Process Steps

STEP 1: User requested to fill their personal details along with a secret key.

1.1 No fields should not ϕ.
1.2 *Secret key<=8digit.*

STEP 2: Image captcha is generated using secret key and random key.

2.1 User image captcha created based on secret key text(red).
2.2 Random image captcha is created and which has an option of refresh.
2.3 Image description.
Height=60.
Width=260.
Surface=white background with black text (concatenated sting of secret and random key).

STEP 3: Image Share creation using VCS.

3.1 Encryption:
Image captcha = share1 + share2.
Share1 ← with user.
Share2 ← Stored in bank database.

STEP 4: Login at Genuine site.

4.1 Decryption:
User ←Enter ID and Share1.
Genuine site ←Retrive Share2

STEP 5: Verification process.

Captcha display ←Share1+Share2.
Image captcha will be revealed only both the Share simultaneously available.

STEP 6: Click that image to send OTP to given contact number. Copy that OTP and enter account page to do safe transaction.

IV. EXPERIMENT RESULTS

The phishing attacks are so common because it can attack globally, capture and store the users confidential information. Security image is created by user, of their own choice. Random key generation algorithm is used to generate a part of key string which has an option of refresh. It is not easy to derive a secret key from image. So the credential details of an user is secured. Instead of password an image is used which is generated, based on an user secret key and the random key. In exiting security image is chosen from the give image, but in proposed a security image is created by user. Random key is fixed but generate only once in existing, but in proposed it is also fixed and has an option of refresh. The generated image is encrypted using VCS. One outcome is given to user for late use of login and another kept in separate storage of bank. At the time of authentication, user ID and image is used. Authoriztion is done at the bank website.

IV. CONCLUSION

In this paper ,we had deal with a critical research issue in phishing for effective online banking management .The research is about anti-phishing based on the concept of Visual cryptography scheme implemented in the registration of online banking system to improve the effectiveness on a security image. This concludes that the password based on an image preference a high effectiveness with easy maintenance. In the future it plan to implement this module in Online web applications. Based on that feedback the tool will be enhance.

REFERENCES

[1] Dao-Shun Wang, Tao Song, Lin Dong, and Ching-Nung Yang,”Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing,” IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12, December 2013.

[2] Engin Kirda and Christopher Kruegel,”Protecting Users Against Phishing Attacks with AntiPhish,”IEEE, 2005.

[3] Feng Liu, Chuankun Wu and Xijun Lin,”Step Construction of Visual Cryptography Schemes,”IEEE Transactions on Information Technology, Vol.5, No.1, March 2010.

[4] Haidong Xia and Jose Carlos Brustoloni,”Hardening web browsers against man-in-the-middle and eaves dropping attacks,”IEEE, May 2005.

[5] Hossain Shahriar and Mohammad Zulkernine,”PhishTester: Automatic Testing of Phishing Attacks,”IEEE Transaction on Computer Society, 2010.

[6] Joel Lee, Lujo Bauer and Michelle L. Mazurek,”The Effectiveness of Security Images in Internet Banking,”IEEE Transaction on Internet computing, January/February 2015.

[7] Kristofer Beck and Justin Zhan,”Phishing in Finance,”IEEE Transaction, 2010.

[8] Min Wu, Robert C. Miller, Simson L. Garfinkel,”Do Security Toolbars Actually Prevent Phishing Attacks,”Computer Science and Artificial Intelligence Lab,Cambridge, 2008.

[9] Wen Qiaoyan, Sun Bin, Liang Xiaoying,”A DNS based Anti-Phishing Approach,”IEEE Transaction on Computer Society, 2010.

[10] Zhang, Gang Liu, Tommy W. S. Chow and Wenyin Liu,”Textual and Visual Content-Based Anti-Phishing: A Bayesian Approach Haijun,”IEEE Transactions on Neural Networks, Vol. 22, No. 10, October 2011.