International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Anti-Phishing Frame-Work applying Visual Cryptography Mechanism

G Lakshmeeswari[†]* and Shubham Goel[‡]

[†]Computer Science and Engineering Department, GITAM University, Visakhapatnam, Andhra Pradesh, India
[‡]Electrical and Electronics Engineering Department, AMITY University, Noida, Utter Pradesh, India

Accepted 01 Jan 2016, Available online 04 Jan 2016, **Vol.6, No.1 (Feb 2016)**

Abstract

In the present risky cyber technology era, network security plays a major role to solve the problems of network resources. Network security consists of services and facilities to prevent and monitor the unofficial access, wrong usage, alterations or denial of computer networks. One of the major problems being faced is phishing, which is fraudulently acquiring confidential and sensitive information. These frauds make Anti-phishing Frame work a necessity so that users cannot be tricked by such a combination of spoofing techniques. Our proposed system supports anti-phishing frame work with the help of visual cryptography. This methodology is used in verifying legitimacy of the server-under-test which is a secure anti-phishing approach using image based validation. It involves storing of a secret image in shares and original image can be obtained only by overlapping those shares

Keywords: *Network security, Phishing etc.*

1. Introduction

The rising internet usage has paved the way for a wide variety of applications. As the usage increased, attacks also increased. With the steep rise of online, their vulnerability to attacks has also increased. Dynamic IP addressing system has added fuel to fire. Phishing is the major security threat identified among them. It is a form of online theft that aims to steal sensitive information such as online banking passwords, credit card information from the user, etc. by masquerading as a trustworthy entity in electronic communication.

Phishing attack is a combination of technical deceit and social engineering practices. In majority of cases the phisher persuades the victim to intentionally perform a series of actions to gain confidential information. There are various types of phishing attacks such as spear phishing, clone phishing, whaling, rouge Wi-Fi, link manipulation, tab nabbing, etc.

The most common communication channels are e-mail, web pages and instant messaging services. In all these cases the phisher manages to impersonate as a trusted source. The most successful phishing attacks have been initiated by email, where the phisher acts as the sending authority (e.g. Spoofing the source email address and embedding appropriate corporate logos).

In this paper we mainly concentrate on link manipulation, here the URL of the original website is modified, where the sub domain names are changed or misspelled which leads to wrong interpretation by the users. Thus the users are tricked to these disguised websites and give their credentials or confidential information to them. We introduce an "Anti-Phishing framework" using visual cryptography mechanism.

2. Visual Cryptography

Visual cryptography was introduced by Naor and Shamir in 1994. This methodology involves encryption of secret image into shares. These shares are binary images usually presented in transparencies. The act of decryption is simply to stack the shares to view the secret image.

The basic model of visual cryptography assumes that the secret message consists of black and white pixels. Each pixel is either divided into two or four subpixels. These subpixels form the shares for the secret message (B Borchert *et al*, 2007). For instance consider a source image P shown below:

Random shares P1 & P2 are produced, such that they do not disclose any information unless and until they are overlapped.

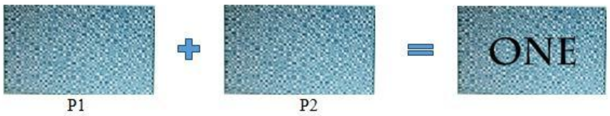

Fig.1 Visual Cryptography

*Corresponding author: **G Lakshmeeswari**

Encryption and decryption using Visual cryptography can be achieved through one of the following schemes:
→(2, 2) Threshold VCS scheme-This scheme involves encryption of a secret image into 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, n) Threshold VCS scheme-This scheme involves encryption of secret image into n shares such that when any two of the n shares are overlaid the secret image is revealed. Here the user will be prompted for n (number of participants).
→(n, n) Threshold VCS scheme- This scheme involves encryption of secret image into n shares such that when all the shares are overlaid the secret image is revealed. Here the user will be prompted for n (number of participants)
→(k, n) Threshold VCS scheme- This scheme involves encryption of secret image into n shares such that when any k shares are overlaid the secret image is revealed. Here the user will be prompted for n (number of participants) and Threshold.

3. Related Works

The work done in this area is mostly concerned with authenticating the server using visual cryptography methodology. Authenticating a server exclusively may not be sufficient to drip free from phishing attacks. Therefore we proposed a system which authenticates the Trusted server and the local server as well.

(Y.Yesu Jyothi,*et al*, 2013) proposed an approach to solve the problem of phishing through textual validation along with visual cryptography scheme. A (2,2) VC scheme is used along with the key entered by the user during its registration with the website.

(A.Angel Freeda, et. al, 2013) proposed a system to identify the phishing website by using image captcha based authentication using visual cryptography. The original image captcha is divided into many blocks and rearrangement is done. The individual shares do not reveal the identity of the original image captcha. Once the original image captcha is revealed, after merging different shares, it can be used as the password.

(B.Padhmavathi *et al*, 2010) proposed a solution to the cheating problem in Visual cryptography by malicious adversaries. The proposed scheme provided authenticity for the VC shares and makes these secret shares invisible by embedding them into not insignificant host images. It is a type of blind watermarking scheme where every pixel of the binary VC share is invisibly embedded into the individual blocks of the host image.

(Bernd Borchert *et al*, 2010) used the version of visual cryptography which is segment based. It is a type of encryption of messages consisting of symbols which can be presented by a segment display. This paper show cases the advantage of the segment-based encryption as being easy in adjusting the secret images and easy for recognition of the symbols for the human eye, especially in a transparency-on-screen scenario.

4. Proposed Methodology

The major entities involved the current scheme are client, Trusted Server (TS) and Server under Test (SUT)**.** A secured methodology is proposed to verify the authenticity of the server using the concept of visual cryptography. This system uses an image-based authentication by decomposing a random image into two shares in a particular session. The trusted-server helps the client in identifying the genuineness of the server-under-test by performing decryption of the shares. It finally determines whether the server-under-test is a legitimate server or not before the client starts accessing that server.

Client

A Client is a user in an organization or a single user who wishes to accesses the trusted server and Server Under Test(SUT) for accessing the information over internet. The client accesses the Server Under Test through the Trusted Server. In this paper we propose a verification of the identity of the SUT also to prevent the phishing attacks. The frequently accessed SUT's are authenticated by the trusted server and authentication of client and trusted server is also done.

The client has to register to the trusted server and authentication between both these parties is done with the assistance of visual cryptographic methodology where an image is selected and split into shares and shared by both the parties. If the original image is overlapped and the appropriate image results, both the parties are authenticated. The same functionalities are explained in detail below:

Client's functions

(i) Registration to the Trusted Server (TS)

- Select a Random image.
- Encrypt the image into two shares(S1, S2).
- Distribute the share (S2) to TS.

(ii) Access

- Receive the share S2 from trusted-server after login.
- Perform decryption with S1 hosted with the client and the received share S2.
- Verify original image with the final decrypted image.
- If there is a match the TS is authenticated and the further process continues or else the request is turned out as Phishing attack.

This process of authentication prevents the phishing of Trusted server.

Trusted-Server

The Trusted Server's functionality is to authenticate the Server under Test. The authentication procedure is similar to that of the client and trusted server authentication. We name the shares used here as S3 and S4. The authentication at this point assures that the SUT is not being phished. The detailed process done by the Trusted Server is listed below:

(i) Registration

- Register the frequently accessed local servers for surfing.*(Process is same as that of client-TS registration)*
- Random image selection.
- Encrypt the image into two shares (S3, S4).
- Distribute the share (S4) to Server Under Test (SUT) and retain S3

(ii) Access

- Receive server-under-test credentials and verify.
- Receive share S4 from server-under-test.
- Decrypt S4 share with its own share S3.
- Verify original image with the decrypted image.
- If there is a match the SUT is authenticated or else it is under stood that an attack has occurred.

This process prevents the phishing of Server Under Test.

Server-Under-Test

- Receive share S4 from TS during registration.
- Send its credentials and the received share to trusted-server during verification process by TS.

The client logs into the server with his username and password (these credentials were obtained during client's registration with the server). After a successful login, the client selects a random image and divides it into two shares (encryption). Share-1 is stored with the client in his database, share-2 is sent to the trusted-server. The Trusted server registers frequently accessed server for surfing. These servers are referred as server-under-test in this paper. The registration process of SUT – TS is similar to that of Client – TS. The TS is authenticates clients and client authenticates TS to assure that TS is not phished. Similarly SUT sends its share along with its credentials to the trusted-server for verification of its genunity .The trusted-server verifies the credentials to check whether the server-under-test has been previously registered to it. If these credentials are accurate trusted server decrypts share-4 and share-3 and thus authenticates the SUT that it is not phished.

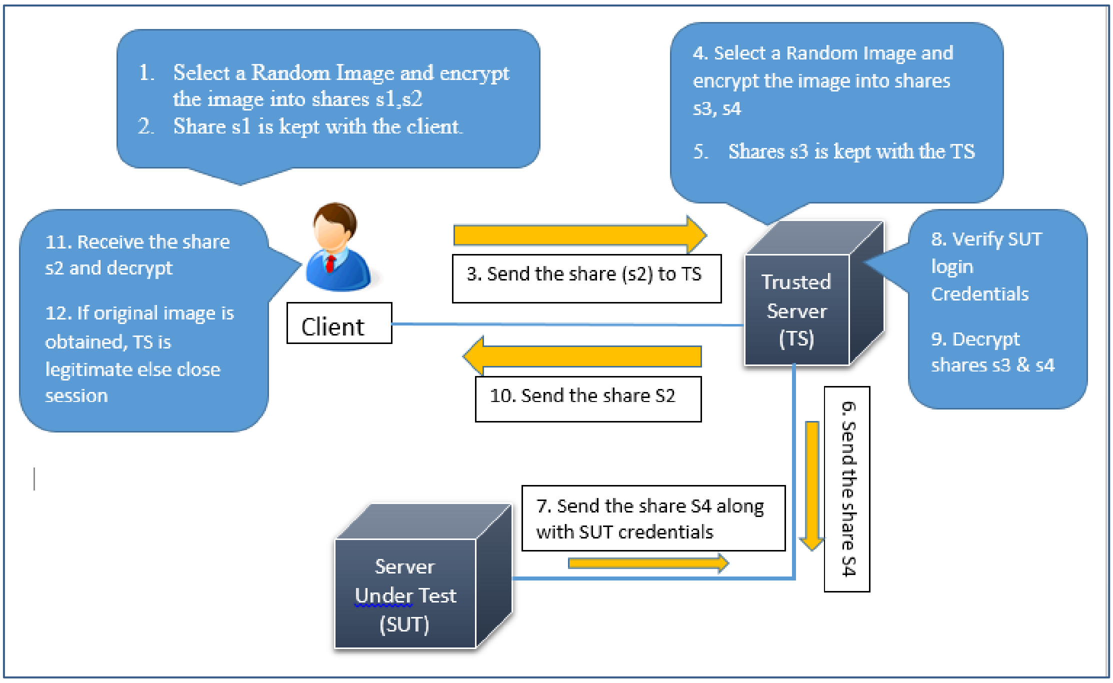
1. Select a Random Image and encrypt the image into shares s1,s2
2. Share s1 is kept with the client.
4. Select a Random Image and encrypt the image into shares s3, s4
5. Shares s3 is kept with the TS
11. Receive the share s2 and decrypt
12. If original image is obtained, TS is legitimate else close session
Client
3. Send the share (s2) to TS
Trusted Server (TS)
8. Verify SUT login Credentials
9. Decrypt shares s3 & s4
10. Send the share S2
6. Send the share S4
7. Send the share S4 along with SUT credentials
Server Under Test (SUT)

Fig.2 Proposed System Model

Conclusions

The proposed methodology helps to be secure online phishing attacks. This methodology assures more security as the visual cryptography technique is applied on a random image selected for every new server-under-test. All the three entities (Trusted-Server, client, Server-Under-Test) are authenticated and assures that every entity is original. This assures that all the entities are protected from being disguised. Performing decryption at two different stages to obtain the final image assures more security. This proposed methodology safeguards the users from phishing attacks. When there are multiple server-under-test's for verification, there is load on the trusted-server for checking credentials of too many server-under-tests. This is a major limitation of this proposed technology. This can be overcome by continuing the session once an SUT is authenticated. Authentication is done only when a new session is to be started.

References

Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar and Prof. S. Baj, (2014), An Enhanced Anti-Phishing Framework Based on Visual Cryptography, *International Journal of Emerging Research in Management &Technology*, Vol. 3, Issue-3.

Anushree Suklabaidya and G. Sahoo, (2013), Visual Cryptographic Applications, *International Journal on Computer Science and Engineering*, Vol. 5 No. 06.

Y.Yesu Jyothi, D. Srinivas and K. Govindaraju, (2013), The Secured Anti-Phishing approach using image based validation, *International Journal of Research in Computer and Communication Technology*, Vol. 2, Issue 9.

A.Angel Freeda, M.Sindhuja and K.Sujitha, (2013), Image Captcha Based Authentication Using Visual Cryptography. *International Journal of Research in Engineering & Advanced Technology*, Vol. 1, Issue 2.

B.Padhmavathi, P.Nirmal Kumar and M.A.Dorai Rangaswamy, (2010), A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography using Image Processing. *International Journal on Signal and Image Processing*, Vol. 1, No.3.

B. Borchert, (2007), Segment Based Visual Cryptography, *WSI Press*, Germany, 2007.

Sonal Wange, (2013), A Visual Cryptography to secure Biometric Database: A Review, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3, Issue-11.

Shital B.Pawar, Prof.NM.Shahana, (2013), Visual Secret Sharing Using Visual Cryptography, *International Journal of Engineering Research* Vol. 3, Issue 1.