DETECTION OF PHISHING E-COMMERCE WEBSITES USING VISUAL CRYPTOGRAPHY

ULKA M. BANSODE¹, PROF. GAURI R. RAO², PROF. Dr. D. M. THAKORE³

¹Department of Computer Engineering, BharatiVidyapeeth Deemed University, College of Engineering, Pune, Maharashtra, India.
²Associate Professor, Department of Computer Engineering, BharatiVidyapeeth Deemed University, College of Engineering, Pune, Maharashtra, India.
³Head of Department, Department of Computer Engineering, BharatiVidyapeeth Deemed University, College of Engineering, Pune, Maharashtra, India
E-mail: Ulka_bansode09@yahoo.co.in

ABSTRACT
Internet has changed the life of human significantly and it has dominated many fields including e-Healthcare, e-Commerce, etc. Internet increases the comfort of human life; on the other hand it also increases the need for security measures too. With the popularity of E-commerce websites various online attacks has been increased one of them is phishing attack.

Phishing is the act of misleading someone into giving confidential information (like passwords and credit card information) on a fake web page or email form pretending to come from a legitimate company (like their bank). Phishing emails may contain links to websites that redirects users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

This paper presents a new approach for detecting phishing E-commerce websites. Visual Cryptography is used for detection of phishing websites. Phishing websites are crafted to closely mimic look and feel of legitimate sites.

Keywords: Image shares, Phishing, Visual Cryptography.

1. INTRODUCTION

The growth of the Internet has allowed users to manage their personal finances and expenditure online. E-commerce and online banking has made life easier. The increase in online services offered to consumers has naturally led to an increase in the exchange of personal information to access such services. With the popularity of E-commerce websites various online attacks has been increased one of them is phishing attack. Phishing has become one of the major issue in recent times. This attack will not hack any server or the website; it just creates duplicate copy of the website and tries to communicate to confuse the user. The major reason for concern in the fact that phishing activity directly hit us as it aims at securing our personal and sensitive information. This personal information can be used for the purpose of committing financial fraud, has become a criminal activity on the Internet.

Criminals targeting user information are able to profit from the increased adoption of online services for many day to day activities including banking, shopping and leisure activities. Many times the sites that closely mimic look and feel of legitimate sites are crafted and promoted on the Internet. As these sites looks like legitimate site, user can login into that site through which intruder can get the sensitive information like Username, Password, Bank account number, Credit/Debit card number etc.

Some of the Examples of Phishing Scams are:

- Sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user for providing private information that will be used for identity theft.
- Sending e-mail message to the user’s as if they won the prize and to deposit the amount they are requested to send the personal information and bank account numbers.
- Sending 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.
So to prevent against phishing attack it is very important to make sure that whether the site you are visiting, gets open from right or truthful source or not? Whether it is asking you to send personal information and bank details again and again? Thus making it easier to detect phishing websites and protect against phishing attack here a new method is introduced which can be used as a safe way against phishing which is named as “Detection of Phishing E-commerce websites using Visual Cryptography”.

In this approach website cross verifies its own identity and proves that it is a genuine website to use bank transaction, E-commerce and online booking system etc. The concept Visual Cryptography is used. Visual Cryptography is a secure method that encrypts an image by breaking it into shares.

2. BACKGROUND

2.1. Phishing Attack:

Phishing consists of sending electronic mail or other form of communications to group of people asking for their personal information like credit card numbers and passwords. Attackers creates the websites that closely look like authorized websites and promotes those websites on Internet. When user login through those websites they are actually redirected to phisher’s database where attacker can get personal information of user like password, account details etc.

![Diagram of Phishing Attack]

**Fig. 1: Phishing Attack**

2.2. Phishing Process:

Phishing attacks are performed with following 4 steps:

1. First the attacker creates a faked web site in a web server. This web site would look similar or even the same as the legitimate web site.
2. Using some tools they send lots of spoofed e-mails to target users in the name of legitimate companies and organizations, trying to convince victims to visit their websites.
3. When the user opening an e-mail and clicked on the spoofed hyperlink the link will redirect them to a web page asking the user to input the required information.
4. Once the users input their information, the phishers will get that information and can do anything they want with this information, including drawing out the money from the users’ account.
2.3. Causes of Phishing:

- No strong authentication at websites of banks and financial institutions
- Misleading e-mails
- No check of source address
- Lack of user awareness

2.4. Effects of Phishing:

- Financial loss to the original institutions
- Internet fraud
- Identity theft
- Loss of Public Trust in the Internet

3. RELATED WORK

The DNS Based Anti-phishing approach [2] includes page similarity assessment, blacklist and heuristic detection. The commonly used anti-phishing approach by browser is blacklist which is DNS based anti-phishing approach technique.

Google Safe browsing, Netscape browser 8.1 and Internet Explorer7 are important browsers which use blacklist to protect users when they are navigating through phishing sites.

Heuristic based anti-phishing technique estimates whether the page has some phishing heuristic characteristics. [4]

For example spoof guard toolbar include heuristic characteristics like checking against previously seen images, host name and checking URL for common spoofing techniques.

Automated Challenge Response Method [3] is an authentication mechanism, which includes generation module from server. This module then interacts with Challenge-Response interface in client and request for response from user. The challenge response module then calls the get response application which is installed in the client machine. Once the challenge response is validated, user credentials are demanded from client and are validated by server to proceed the transaction. This method ensures two way authentications, simplicity and also prevents man in middle attack.

Cryptography is one of the best known technique to protect data. Cryptography is sending and receiving encrypted messages that can be decrypted by sender or receiver.

Visual Cryptography schemes were introduced by Naor and Shamir [5] is a simple and secure way to allow the secret sharing of images without any cryptographic computation.

Visual Cryptography for Print and Scan Application [7] suggested by W-Q Yan, D. Jin can be applied for printed text and images only.

A Segment Based Visual Cryptography suggested by Borchert [6] can encrypt only the messages containing symbols, amount and numbers like bank account number.

4. VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

Following are the Visual Cryptography Schemes:

1. \((n, n)\) visual cryptography:
   In this type of visual cryptographic scheme, the system generates \(n \geq 2\) number of shares and all shares are needed to be stacked together to get back the secret information.

2. \((k, n)\) visual cryptography:
   In this type of visual cryptographic scheme, the system generates \(n \geq 2\) number of shares and at least any \(k\) \(2 \leq k \leq n\) shares are needed to regenerate the secret information.

3. \((2,2)\) visual cryptography:
   In this type of visual cryptographic scheme, the system generates 2 shares and the secret information will be regenerated after stacking these two shares.

The proposed approach uses \((2,2)\) VCS, each pixel \(P\) in the image is encrypted into two subpixels called shares. The following figure denotes the shares for a white and black pixel. Here choice of shares for black and white pixel is randomly determined. When these two shares are stacked, the value of the original pixel \(P\) can be determined.
5. SYSTEM ARCHITECTURE

Here a new approach is proposed for detection and prevention against phishing attack. This approach is based on visual cryptography. It prevents confidential information from the phishing websites.

The proposed approach is divided into two phases:

5.1. Registration Phase:

In registration phase, user will provide the profile information and sends registration request to trusted server for example bank server. After receiving registration request server will generate public/private key pair. Public key is propagated to the user; private key will never leaves the server.

Key pair and user details are saved in the database of trusted server. After registration, the user can change the key pair any time later. Registration process is depicted in Figure 4.

5.2. Server Verification Process (Phishing Website Detection):

In proposed approach server verification process considers two servers. One server is ‘Trusted Server’ for e.g. Bank Server and another server is ‘Server Under Test’ for e.g. Merchant Server. ‘Server under Test’ can be either registered server or unregistered server. List of authorizes servers is kept in the database of Trusted Servers.

At the time of login user will be prompted for username and key provided by the Trusted Server. Then user is asked to select image. After loading an image, Visual Cryptography is applied to an image and two shares are generated as share1 and share2. Share1 is encrypted and transmitted to ‘Server UnderTest’ (Merchant Server). The ‘Server UnderTest’ sends this encrypted share along with its own details to ‘Trusted Server’. ‘Trusted Server’ provides decrypted version of the share1 only if ‘Server Under Test’ is registered with ‘Trusted Server’. Otherwise it will send any garbage share.

‘Server UnderTest’ will receive this decrypted share1 and retransmits it back to the client. At the client side, client will regenerate image by stacking new share1 and old share2.

If stacking of these shares results into an original image then it is secure website otherwise it is phishing website.

The Server Verification Process is depicted in Fig. 5.
6. **ALGORITHM**

Step 1. User will login and select an image randomly.

Step 2. Perform cryptography and convert the image into shares.

Step 3. Encrypt one of the shares and send to ‘Server Under Test’.

Step 4. Retransmit encrypted share along with own details to ‘Trusted Server’.

Step 5. Compare ‘Server Under Test’ with list of registered servers.

Step 6. If ‘Server Under Test’ is registered server, then perform decryption and send decrypted share to ‘Server Under Test’, and go to Step 8.

Step 7. If ‘Server Under Test’ is not a registered server, then ‘Trusted Server’ will send any garbage share to ‘Server Under Test’.

Step 8: Retransmit decrypted share to client.
Step 9: At client side, both these shares are stacked together. If stacking of the shares results in an original image as was selected at the time of login then go to Step 10 else go to Step 11.
Step 10: Inform client as ‘Not a phishing website’, go to Step 12.
Step 11: Inform client as ‘Phishing Website’, go to Step 12.
Step 12: Stop.

7. RESULTS

This software is tested with 2 registered servers and 1 unregistered server; these servers can be considered as ‘Server UnderTest’. While login user will select an image and will click ‘create shares’ shares will be generated as shown in the Fig. 6 and then click ‘Verify Server’ button.

If the ‘Server UnderTest’ is genuine/true server then stacking of the shares will result in an original image as shown in Fig. 7.

If the ‘Server UnderTest’ is not a genuine/true server then stacking of the shares will result in any unrecognizable image share as shown in Fig. 8.

8. CONCLUSION
This paper presents a new approach for detection of phishing E-commerce websites. Visual Cryptography is used as a solution for detecting phishing websites. With the help of VC, the security of E-commerce website has been increased. The proposed methodology preserves confidential information of the users and it verifies whether the website is genuine/true or phishing website. If the website is phishing website, then in that situation phishing website can’t display original image selected by user. The users are more secure because the system prevents intruder’s attack on user account and also users are able to update keys at every login.
The proposed methodology prevents attacks on financial web portals, online shopping market and banking portal.

REFERENCES