A Paper on Various Techniques to Overcome Hazards Caused by Phishing Attack

K. Brunda[1], Dr.K. Raghuveer[2]

[1]*M. Tech, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India*
[2] *Professor and Head of the Department, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India*

---***---

Abstract - *Phishing is an endeavor by an individual or a gathering to steal individual confidential information such as, passwords, credit card data and so forth from clueless casualties for wholesale fraud, monetary profit and other fraudulent activities. This paper concentrates on the phishing assaults which incorporates investigation of various commitments of late research on phishing detection and prevention techniques.*

Key Words: **Phishing, Visual Cryptography, Shares, One Time Password (OTP), Authentication, Security**.

1. INTRODUCTION

These days, online exchanges have turned out to be extremely normal and there are a few assaults exhibit behind this. In these sorts of different assaults, phishing is distinguished as a noteworthy security danger which is being confronted by many individuals. Web based keeping money and web based business clients are likewise confronting the issue of phishing tricks. Hence there is a high need of security and preventive instrument ought to be considered adequately.

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. For malicious reasons, by disguising as a trustworthy entity in an electronic communication. Phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in current web security. One definition of phishing is given as "it is a criminal activity using social engineering techniques". Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details by masquerading as a trustworthy person or business in an electronic communication [1].

The Fig-1 shows the three components namely mail sender which sends large volume of fraudulent emails, collector which collects sensitive information from users, and casher which uses the collected sensitive information to en-cash

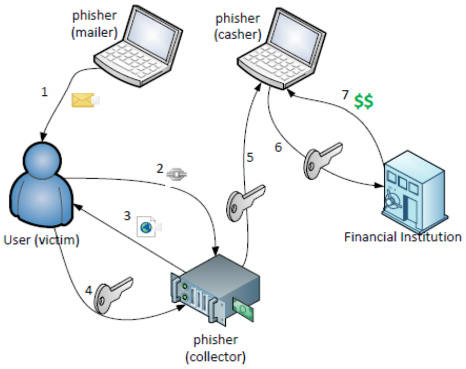


Fig-1: An example for phishing attack

1.1 Why should we care about phishing?

By email, attackers use phishing to get access to our sensitive and confidential information. It is common practice for the attackers to impersonate a trusted person or company in an attempt to collect enough information to steal our identity or confidential information from our employer. These emails can also include attachments that can contain malware that can affect our computer when clicked on. Attackers are very sophisticated these days and can easily set up bogus websites that steal your information without we even realizing it or we realize it too late. For example, an attacker can send you a link to a very real looking but "fake" website, prompting you for information (i.e. name, address, telephone, bank account information, credit card information, social security number) that they can use for personal gain.

2. TYPES OF PHISHING ATTACK

Clone Phishing: A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address taken and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a re-send of the original or an updated version to the original.

This technique could be used to pivot from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Spear Phishing: While traditional phishing uses a 'spray and pray' approach, meaning mass emails are sent to as many people as possible, spear phishing is a much more targeted attack in which the hacker knows which specific individual or organization they are after. They do research on the target in order to make the attack more personalized and increase the likelihood of the target falling into their trap.

Email/Spam Phishing: Using the most common phishing technique, the same email is sent to millions of users with a request to fill in personal details. These details will be used by the phishers for their illegal activities. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, or verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email.

Web Based Delivery: Web based delivery is one of the most sophisticated phishing techniques. Also known as “man-in-the-middle,” the hacker is located in between the original website and the phishing system. The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.

Whaling: Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

3. VISUAL CRYPTOGRAPHY

Visual Cryptography(VC) is one of the cryptography strategy which was right off the bat proposed by Naor and Shamir which enables any visual data to be scrambled such that the decoding can be performed by the human visual framework neither any calculation required. The unscrambling procedure takes out the calculation issue. Mystery picture is uncovered by stacking operation implies stacking the offers. Visual cryptography is exceptionally secure, simple to actualize and particularly helpful for the low calculation stack necessity.

4. RESEARCH WORK

4.1 Advance Phishing Detection Using Visual Cryptography and One Time Password

Advance Phishing Detection Using visual cryptography and OTP system aims at providing the facility to detect whether the site is phishing or not and will solve the problem of identity theft and phishing attack [2]. Phishing is an act in which a user’s certifications are stolen, for example, username, watchword, Visa subtle elements and so on for malignant reasons. In this framework both the merchant and the client are registered to the bank and both are verified by the bank server. The OTP is gotten at the client end just when the client and the merchant put their shares. OTP is confirmed by the bank server and if the OTP is legitimate the trader server is recognized against phishing.

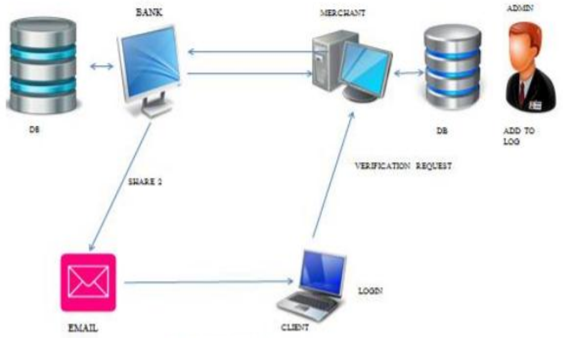


Fig -2: Proposed methodology

The Fig-2 shows the proposed methodology for detection of phishing website. This will keep a customer from being one of the victims of the phishing attack. According to this methodology first of all user and the merchant should be registered to the the bank. Once the user is enrolled to the bank he then can login through the client application utilizing username, password and url of the merchant sites. The verification request is sent to the merchant server. The merchant will then send its server key, server id, uid to the bank. Bank will check the subtle elements that are substantial or not. In the event that its legitimate then it will produce otp generally junk will be created. After that QR will be created and visual cryptography is applied. Share 1 is sent to the merchant and other share will be sent to the client through email. Merchant and client will put their shares at client application. Both the share combines to give the OTP. In the event that OTP get created enter the otp for confirmation the bank server will check the entered OTP. On the off chance that the entered OTP is substantial then the merchant sites is non phishing else it is phishing. Consequently from this technique the client can decide the site is protected or not to complete the exchange.

The advantages of this proposed system are [2]:

1. Authentication: - Client and merchant server are authenticated by the bank server and OTP is also verified by the bank Server.
2. This system protects the customer from man in middle attack.
3. Security: - Customer information is not shared to the merchant until the merchant server is verified.

4.2. A Novel Anti Phishing Framework Based On Visual Cryptography

In this paper another approach named as "A Novel Anti phishing structure in view of visual cryptography" to take care of the issue of phishing has been proposed. Here a picture based verification utilizing Visual Cryptography (vc) is utilized. The utilization of visual cryptography is investigated to safeguard the protection of picture captcha by breaking down the first picture captcha into two offers that are put away in partitioned database servers with the end goal that the first picture captcha can be uncovered just when both are all the while accessible. The individual sheet pictures don't uncover the personality of the first picture captcha. Once the first picture captcha is uncovered to the client it can be utilized as the secret key.

The proposed approach can be divided into two phases:
A. Registration Phase

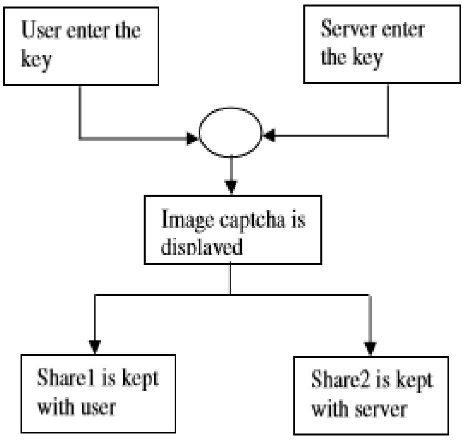


Fig-3: When user performs registration process for the website

The Registration phase is depicted in Fig-3 [1]. In the registration phase, a key string (secret key) is asked from the user at the time of enlistment for the protected site. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated [1]. The image captcha is partitioned into two shares to such an extent that one of the shares is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase [1]. The image captcha is additionally put away in the real database of any classified site as private information. After the registration, the user can change the key string when it is required.
B. Login Phase

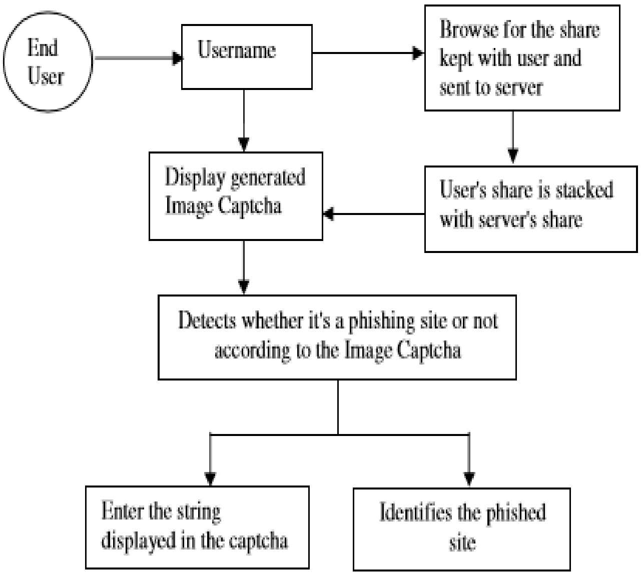
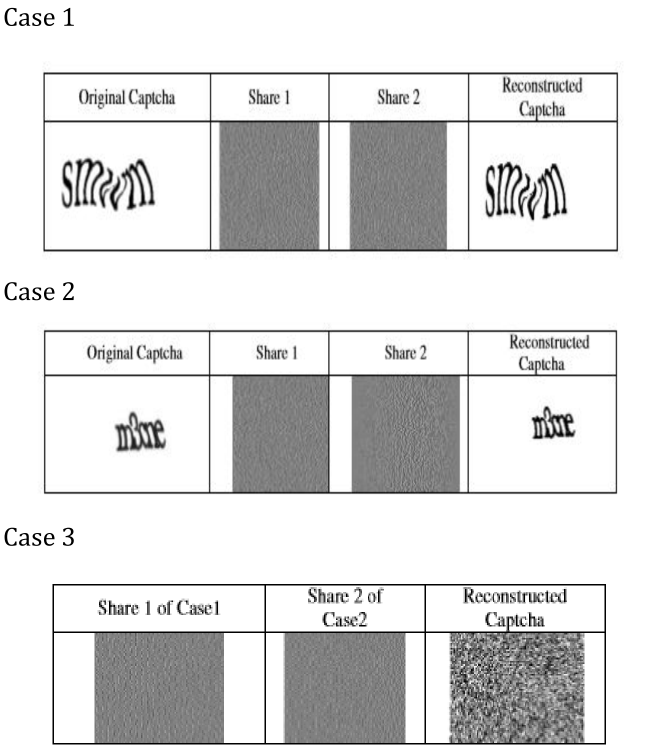

End User
Username
Browse for the share kept with user and sent to server
Display generated Image Captcha
User's share is stacked with server's share
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the captcha
Identifies the phished site

Fig-4: When user attempts to log in into site

The Fig-4 [1] illustrates the login phase. In the Login phase first the user is incited for the username (user id).Then the user is made a request to enter his share which is kept with him. 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 produce the image captcha [1]. The image captcha is shown to the user. Here the end user can check whether the showed image captcha matches with the captcha made at the time of registration. The end user is required to enter the content shown in the image captcha and this can fill the need of password and utilizing this, the user can sign in into the website. Utilizing the username and image captcha created by stacking two offers one can confirm whether the site is real/secure site or a phishing site and can likewise check whether the user is a human user or not.

They have implemented the proposed methodology using Matlab. Fig-5 shows the result of creation and stacking of shares.


Case 1

Case 2

Case 3

Fig-5: Creation and stacking of shares

The entire process is depicted in Fig-5 as different cases. Case1 and Case 2 illustrate the creation and stacking of shares of two image captcha's resulting in original captcha. In Case3 share1 of first image captcha is combined with share2 of second captcha resulting in unrecognizable form of captcha [1].

4.3 Online Payment System using Steganography and Visual Cryptography

This paper presents another approach for giving constrained data just that is essential for reserve exchange amid internet shopping along these lines protecting customer information and expanding customer certainty and preventing identity theft. The strategy utilizes combined utilization of steganography and visual cryptography for this reason.

In this paper, a new method is proposed, that utilizations text based steganography and visual cryptography, which limits data sharing amongst customer and online merchant however empower effective store exchange from buyer's record to shipper's record along these lines defending shopper data and counteracting abuse of data at vendor side. The technique proposed is particularly for E-Commerce yet can undoubtedly be reached out for online and also physical keeping money.

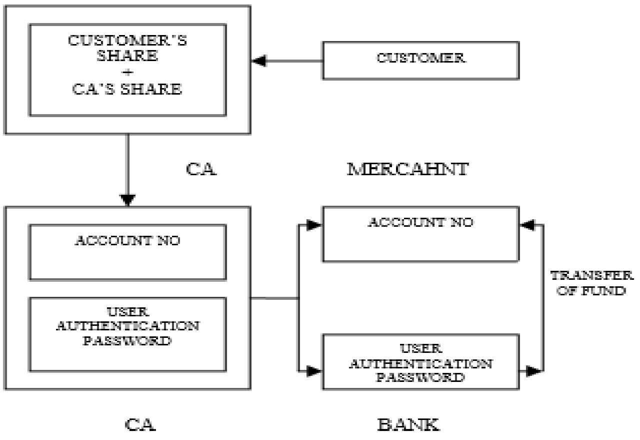

CUSTOMER'S SHARE + CA'S SHARE
CUSTOMER
CA
MERCAHNT
ACCOUNT NO
ACCOUNT NO
TRANSFER OF FUND
USER AUTHENTICATION PASSWORD
USER AUTHENTICATION PASSWORD
CA
BANK

Fig-6: Proposed payment method

In the proposed method, customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method. Customer validation data (account no) regarding merchant is placed over the cover message in its unique frame. Presently a depiction of two texts is taken. From the snapshot image, two shares are generated using visual cryptography. Now one share is kept by the customer and the other share is kept in the database of the certified authority [3]. During shopping online, after choice of wanted thing and adding it to the cart, favored installment arrangement of the merchant directs the customer to the Certified Authority portal. In the portal, customer presents its own share and merchant presents its own particular record points of interest. Now the CA combines its own share with shopper's share and obtains the original image. From CA now, merchant account details cover text sent to the bank where client confirmation password is recovered from the cover text. Customer confirmation data is sent to the merchant by CA. After accepting customer confirmation password, bank matches it with its own database and subsequent to checking legitimate customer, exchanges finance from the customer record to the submitted merchant account. After receiving the funds, merchant's installment framework approves receipt of installment utilizing customer validation data.

The advantage of proposed system is that this strategy limits client data sent to the online merchant. So if there should be an occurrence of a rupture in merchant's database, client doesn't get influenced. It also prevents unlawful use of customer information at merchant's side. Usage of steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy [3].

4.4 Preventing Phishing Attacks Using Anti-Phishing Prevention Technique

In this paper, an Anti-Phishing Prevention Technique namely APPT has been proposed, which depends on the idea of anticipating phishing assaults by using combination of one time random password and encoded (encrypted) token for user machine distinguishing proof. The strategy begins by retrieving the password by SMS or by alternate emails. During login the end user request for the password to the server, in that request it contain of encrypted token. On the off chance that the end client is substantial the password with encrypted token will be send through SMS or EMAIL. By using the login id and OTP password user can access the website. For generating encrypted token, x.509certificate2 uses IP address to generate and it's been encrypted by RSA algorithm [4]. The Figure shows the system architecture of the proposed methodology.

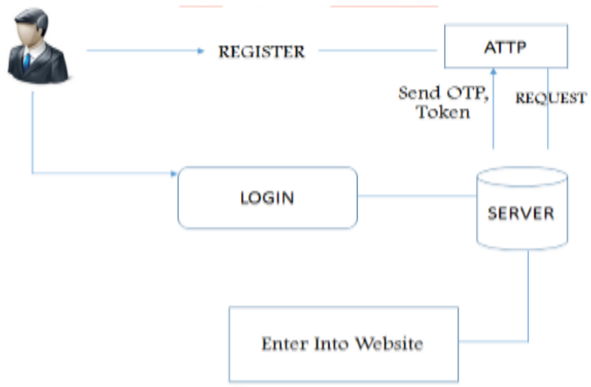


Fig-7: System Architecture

One-time passwords can be generated in several ways and each one has different benefits in terms of security, convenience, cost and accuracy. A more helpful route for users is to utilize an OTP token which is a hardware device capable for producing otp.

If attacker creates a forged website for getting the one tme password, he/she will not be able to cause any damage as the site is only used to retrieve the password on mobile or email which is only accessible to the valid user. In order to mitigate against the Cookie attack, the token (cookie) expires in 15 minutes and the cookie is transmitted over encrypted channel and is also encrypted with X.509Certificate2 certificate [4]. By making a fashioned site the aggressor misdirects the casualties to give certifications (OTP). The client qualifications are recovered by the aggressor keeping in mind the end goal to get to the delicate site. When assailant tries to get to the site with the recovered client certifications, the substantial token (treat) and other machine ID parameters are checked which are not legitimate and in this manner get to is denied. The client accreditations are promptly set to terminate with a specific end goal to stop the replay assault. Because of expiry time of token and one time secret key it will be exceptionally hard to dispatch a fruitful assault.

5. CONCLUSION

The issue of Phishing does not have a single solution as of today. Phishing is not only a specialized issue and Phishers would keep thinking of better approaches for attacking the users. Online users should undertake periodic vulnerability analysis to identify and plug weaknesses that can lead to a successful Phishing attack. To prepare for these dangers, user should be educated on the threats of advanced malware and the structures it can take today. In this paper, we have tried providing an overview on how to solve the problem of phishing attack and techniques used to overcome the phishing attacks. We advise web managing an account administrations to genuinely inquire about these issues before assaults are done in nature. A control that ensures all essential web saving money movement and the data required in this action is required.

REFERENCES

[1] Divya James, 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] Prof N.R.Jain ,Kashid Ujwal , Shaikh Apsara, Patel Nikhil, Divekar Tejashri, "Advance Phishing Detection Using Visual Cryptography and One Time Password", IJARSET Vol. 3, Issue 4 , April 2016.
[3] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.
[4] Gladston Chelliah.A, Aruna.S, Preventing Phishing Attacks Using Anti-Phishing Prevention Technique, 2014 IJEDR Conference Proceeding (NCETSE-2014).
[5] Archit Shukla, Lalit Gehlod, "A survey on phishing detection and prevention technique", International Journal of Engineering and Computer Science Volume 3 Issue 5 may, Page No. 6255-6259.