

Secure Server Verification by using Encryption Algorithm and Visual Cryptography

Shreya Zarkar¹, Sayali Vaidya², Achal Bharambe³, Arifa Tadvi⁴, Tanashree Chavan⁵

¹ Department of Computer Engineering Modern Education Society's College of Engineering Pune, India

² Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

³ Professor, Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

⁴ Modern Education Society's College of Engineering, Department of Computer Engineering Pune, India

⁵ Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

Abstract: In the area of the internet, various online attacks have been increased day by day and among them the most popular attack is phishing which is done by hackers or unauthorized users. Phishing is an attempt by an individual or a group to acquire personal confidential information such as passwords, credit card information etc. from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Hackers host similar website to misguide the user and store the confidential information of the user to their own website by providing link. Without proper safeguards, applications are vulnerable to various forms of security attack. Thus it is very important for the users to identify the fake and genuine website. Thus the online security is major part websites. In this paper we have proposed a new approach for the identification of genuine server named as "Secure Server Verification by Using RSA Algorithm and Visual Cryptography" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (VC) is used and the encryption algorithm is used.

Keywords: phishing, authentication, security, theft, safeguard, confidential.

1. Introduction

Now days, Online transactions are very common and various online attacks are present behind this. Phishing is one kind of attack in which confidential and sensitive information can be gained by the attackers. Phishing [1] is identified by major attack among all online attacks and new innovative ideas are arising with this. Thus, security in such cases should be very high which cannot be tractable by implementation easiness. Phishing can be defined as "it is a criminal activity using social engineering techniques". Attackers host a website which is similar to the banking website and attackers bombard mails to some random users. The mail format and GUI is exactly similar to the banking mails. They request the users to update their password for the safety .the mail contains the URL which redirects the users to the fake website. Attackers use the replica of the original website misguiding the user that it is a banking website or a government website. Users fill in the confidential information and attackers pull the information to their own illegal website. Thus users fall prey to these kinds of fake mails and expose their user id and password. The attacker takes the advantage of it. After collecting this confidential information from the user they log in to the actual banking website with the help of the login id and password provided by the user and they transfer the money from the users account to their account. Thus phishing is the indirect way of stealing money online from the user. There is extreme need of online security to the legal websites. In general, the phishing attacks are performed with the following four steps:

1. Attacker sets up a phishing site, which looks like the legal website.
- 2) Phisher then sends the link of the website to the large number of spoofed e-mails in order to catch the user's information in the name of legal organizations, companies, government sectors, trying to convince the users to visit their website.
- 3) Victim then visits the fake website by clicking on the link and inputs its useful information.
- 4) Phisher then steals the information and performs their fraud such as transfer of money from victims account.

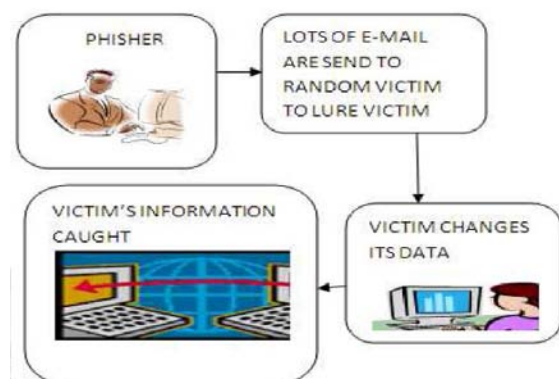


Figure1: Process of Phishing

2. Classification of Phishing Attacks

Phishing attacks can be classified into following types according to the way attack is done.

2.1 Deceptive phishing

In this type of phishing attacker broadcasts an email such as message regarding need to verify account information, reenter users information because of system failure, undesirable account changes, new free service, and may other scams ,with the hope that victim will enter their information and caught in to attackers trap.

2.2 Malware based phishing

This type of attack involves running malicious software on victim’s pc, malwares can be introduced as email attachment, or in downloadable file from website, or by exploiting security vulnerabilities.

2.3 Web Trojans

This kind of attacks pops up invisibly when users attempt to log in. They collect users’ information locally and transmit to the phisher.

2.4 System reconfiguration attack

In this type of attack users pc configuration is changed for malicious purpose to redirect users to the URL look alike, for example the Banks URL may be changed from www.gmail.com to www.gmail.com, we can see here l is replaced by 1.

2.5 Man in middle phishing

In this type of phishing attacker puts themselves between the user and legal website, they record the user’s information and continue to the legal website so that user can not identify, user’s transactions are also not affected. Later the sell or use the user’s information when user is not active on the system.

2.6 Search engine phishing

In this type of phishing attacker creates very much attractive website with sound effects, so when users do normal search they find such kind of website and are fooled by giving up their information. To overcome these We are going to use a secure server verification using approach named as "Secure Server Verification by Using RSA Algorithm and Visual Cryptography" i.e. every user request will be redirected from web server to secure server and their credentials are matched with the server credentials and upon verification of the credentials the user verifies the server and the transaction is started.

3. Visual Cryptography

Cryptography is the commonly used technique to protect the data. In this technique messages are encrypted and that can be decrypted by only the intended sender or the intended receiver. Various mathematical algorithms are used for encryption and decryption in such a way that no one but the intended recipient can decrypt and read the message. Visual cryptography scheme (VCs) is introduced by Naor and

Shamir [2]. It is a simple and secure way to allow the secret sharing of images. An image is composition of pixels. The shared secret is an image composed of black and white pixels. Let each pixel be stored in bits. Then 2d gray-leveled image can be shown by using a set of pixels. A recursive VC method proposed by monoth et al., [3] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. Similarly a technique proposed by Kim et al., [4] also suffers from computational complexity, though it avoids dithering of the pixels. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [5], [6], [7]. In these cases all participants will not present false or fake shares during the phase of recovering the secret image. Thus, the image shown on the stacking of shares is considered as the real secrete image.

Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

- 1)(2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes 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 VCS 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 VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image is revealed. The user will be prompted for n, the number of participants.
- 4)(k, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the Threshold, and n, the number of participants.


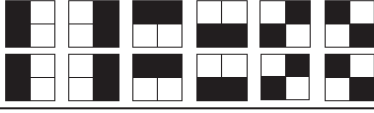


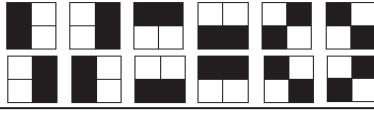

 white pixel p	share 1 block share 2 block	
decrypted pixel		
 black pixel p	share 1 block share 2 block	
decrypted pixel		

Figure 2: 2-out-of-2 VCS scheme with 2 sub pixel constructions

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig 2 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly

determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

4.1 Registration Phase

In the registration phase the most important part is the creation of shares from the image where one share is kept with the user and other share can be kept with the server. If server under test sends some different share then the stacking of shares will create unrecognizable form of image. The stepwise procedure is shown in the figure 3.

4. System Architecture

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. The proposed approach can be divided into two phases

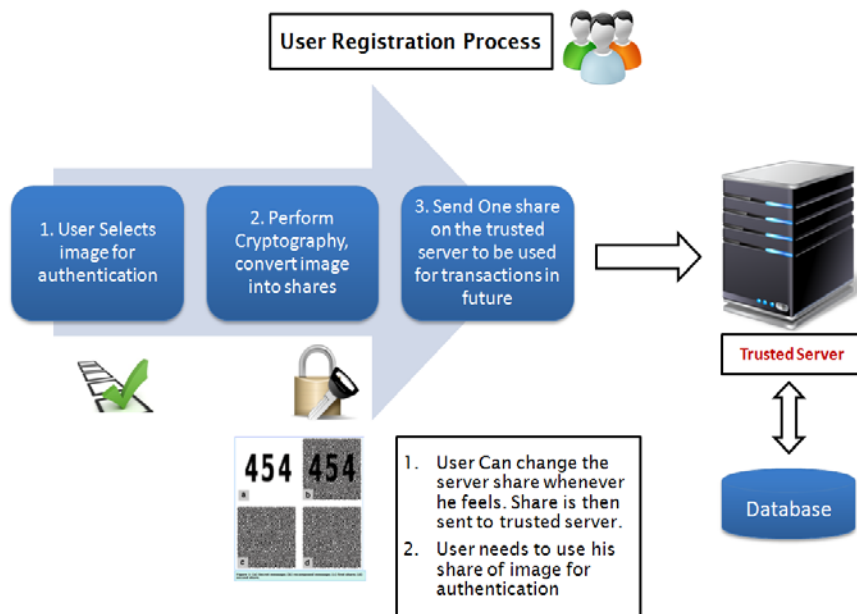


Figure 3: Registration Phase

4.2 Login Phase

In the login phase the user has to enter the user id and his share of image with the public key. The user id, share of image and public key is sent to the server and they are decrypted using the public and private key of the user. At the

server side both the share of images (server share and user share) are stacked together to form the original image. This original image is sent to the user's browser window. Now the user will understand that this is the trusted server and user can enter his further credentials. The stepwise procedure is shown in the figure 4.

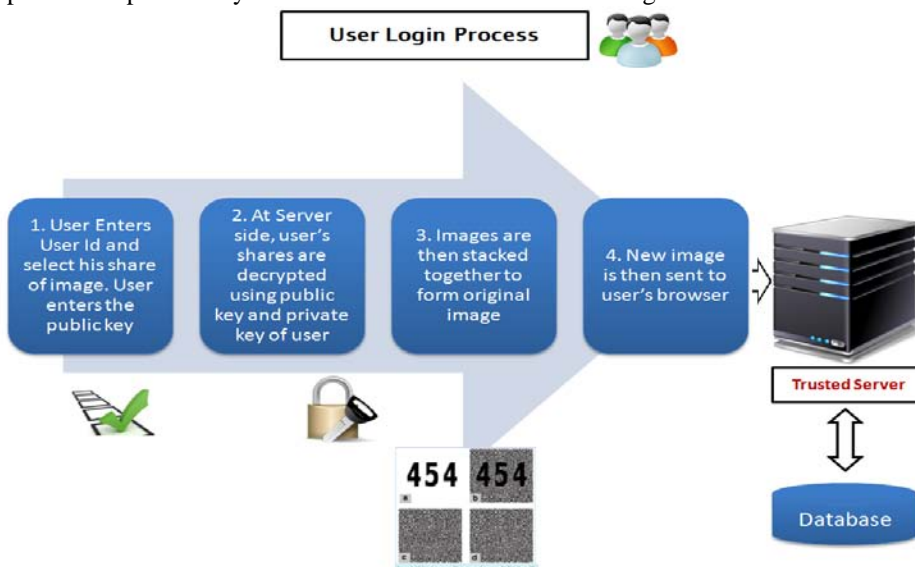


Figure 4: Login Phase

5. Implementation

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997. The user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem. Here are the steps for finding the public and the private key

5.1 Key Generation

- 1) Select two large prime numbers p, q
- 2) Compute
 - $n = p \times q$
 - $v = (p-1) \times (q-1)$
- 3) Select small odd integer k relatively prime to v $\text{GCD}(k, v) = 1$
- 4) Compute d such that
 - $(d \times k) \% v = (k \times d) \% v = 1$
- 5) Public key is (k, n)
- 6) Private Key is (d, n)

5.2 Encryption and Decryption

- 1) Alice and Bob would like to communicate in private
- 2) Alice uses RSA algorithm to generate her public and private keys
 - Alice makes key (k, n) publicly available to Bob and anyone else wants to send her private messages
- 3) Bob uses Alice's public key (k, n) to encrypt message M :
 - compute $E(M) = (M^k) \% n$
 - Bob sends encrypted message $E(M)$ to Alice
- 4) Alice receives $E(M)$ and uses private key (d, n) to decrypt it:
 - compute $D(M) = (E(M)^d) \% n$
 - decrypted message $D(M)$ is original message M
- 5) RSA algorithm for encryption/decryption
 - encryption: compute $E(M) = (M^k) \% n$
 - decryption: compute $D(M) = (E(M)^d) \% n$
- 6) With the help of RSA algorithm the public and private keys can be generated and thus used for encryption and decryption.

6. Conclusion

With the huge use of internet phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing

process. Phishing is mainly done to gain the access to confidential information. Phishing websites as well as human users can be easily identified using our proposed "Secure Server Verification by using Encryption algorithm and Visual Cryptography". Thus with help of these techniques we can successfully help the users to identify the fake and genuine website.

7. Acknowledgment

The authors gratefully acknowledge the contributions of Naor and A. Shamir for their work in the field of visual cryptography.

References

- [1] Ollmann G., the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
- [2] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1-12.
- [3] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion., in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.
- [4] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, .An Innocuous Visual Cryptography Scheme., In Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
- [5] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes., In Journal on Cryptography, vol. 12, 1999, pp. 261-289.
- [6] P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with specied Whiteness Levels of Reconstructed Pixels., Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.
- [7] 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.

Author Profile

Shreya Zarkar is a graduate student from Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

Sayali Vaidya is a graduate student from Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

Achal Bharambe is Professor from Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

Arifa Tadvi is a graduate student from Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India

Tanashree Chavan is a graduate student from Department of Computer Engineering, Modern Education Society's College of Engineering Pune, India