International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Secure Server Verification By Using RSA Algorithm And Visual Cryptography

Aboli Bhanji
AISSMS's COE, Maharashtra
India

Priyanka Jadhav
AISSMS's COE, Maharashtra
India

Sayali Bhujbal
AISSMS's COE, Maharashtra
India

Punam Mulak
AISSMS's COE, Maharashtra
India

Abstract —
In the era of the internet, various online attacks have been increased and among them the most popular attack is phishing. 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. In this paper we have proposed a new approach 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. Trusted server stores unique keys for users required for encryption and decryption of images.In registration process select random image. After that perform cryptography and convert image into two shares. Send one share after encryption to trusted server for the tests. Provide encrypted version of share only if server under test is registered with trusted server. Send share back to client. Receive the share and perform decryptography to obtain a image. If this image is same as original image then the website can be used for further transaction.

Problem Statement:

1: Phishers can fake the URL that appears in the address field at the top of user's browser window and redirect him to another web site with the intention of performing fraud.

2. Fraudsters send e-mails with a link to a spoofed website asking you to update or confirm account related information. This is done with the intention of obtaining sensitive account related information like your Internet Banking User ID, Password, PIN, credit card / debit card / bank account number, card verification value (CVV) number, etc.

***Keywords*- Phishing, visual cryptography, RSA, shares, Security**

I. INTRODUCTION

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic_communication. The probability of an online shopper coming across a phishing website is alarmingly high.

Phishing emails may contain links to websites that are infected with malware[1]. To deceive users into thinking phishing sites are legitimate, fake pages are often designed to look almost the same as the official ones in both layout and content. In addition, phishers might insert an arbitrary advertisement banner that redirects users to another malicious Web site if they click on it. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the original one. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Thus the security in these cases be very high and should not be easily tractable with implementation easiness.

One definition of phishing is given as "it is a criminal activity using social engineering techniques". Another comprehensive definition of phishing, states that it is "the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft"[2]. In the majority of cases the phishers must persuade the victim to intentionally perform a series of actions that will provide access to confidential information. Communication channels such as email, web-pages and instant messaging services are popular. In all cases the phisher must pretend as a trusted source (e.g. the helpdesk of their bank, online shopping etc.) for the victim to believe. To date, the most successful phishing attacks have been initiated by email – where the phisher pretends to be the sending authority. For example, the victim receives an email supposedly from apps@mybank.com (address is spoofed) with the subject line 'security update', requesting them to follow the URL www.mybank-validateinfo.com (a domain name that belongs to the attacker – not the bank) and provide their banking information.

So we introduce a new method which can be used as a safe way against phishing which named as "Secure Server Verification by Using RSA Algorithm and Visual Cryptography ". As the name describes, 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.) before the end users provide any confidential information and make both the sides of the system secure as well as an authenticated one.

II.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 [3]. 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'd' bits. Then 2^d gray-leveled image can be shown by using a set of pixels. A recursive VC method proposed by Monoth et al., [5] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. Similarly a technique proposed by Kim et al., [6] 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 [7], [8]. 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.

We can achieve this by one of the following access structure schemes [10][11].

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 be 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.

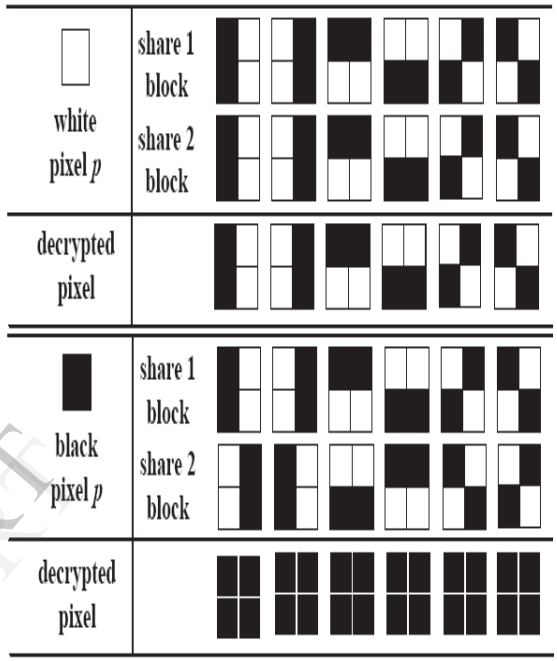

Fig. 1 Illustration of a 2-out-of-2 VCS scheme with 2 sub pixel construction.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.1 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.

III. RSA ALGORITHM

The RSA algorithm was publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters RSA are the initials of their surnames, it is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. As the telecommunication network has grown explosively and the internet has become increasingly popular, security over the network is the main concern for further services like electronic commerce. The fundamental security requirements include confidentiality, authentication, and data integrity. To provide such security services, most systems use public key cryptography. Among the various public key cryptography algorithms, the RSA cryptosystem is the best known, most versatile, and widely used public key cryptosystem today.

Key Generation Algorithm

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integer p and integer q should be chosen at random, and should be of similar bit-length.
2. Compute n = pq.
   - n is used as the modulus for both the public and private keys
3. Compute φ (n) = (p – 1) (q – 1), where φ is Euler's totient function.
4. Choose an integer e such that 1 < e < φ (n) and greatest common divisor of (e, φ (n)) = 1; i.e., e and φ (n) are co-prime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption .
5. Determine d as:

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

   i.e., d is the multiplicative inverse of e mod φ (n).

   - This is more clearly stated as solve for d given (de) = 1 mod φ(n)
   - d is kept as the private key exponent.

By construction, d*e= 1 mod φ(n). The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of

the modulus n and the private (or decryption) exponent d which must be kept secret. (p, q, and φ(n) must also be kept secret because they can be used to calculate d.)

Encryption

Sender A does the following:-

- Obtains the recipient B's public key (n, e).
- Represents the plaintext message as a positive integer m such that

$$0 \leq m < n.$$

  Computes the cipher text

$$c = m^e \pmod{n}.$$

- Sends the cipher text c to B.

Decryption

Recipient B does the following:-

- Alice can recover m from c by using her private key exponent d via computing

$$m = c^d \pmod{n}.$$

- Extracts the plaintext from the integer representative m.

IV. CURRENT METHODOLOGY

We often do online transactions like mobile recharge, online shopping from websites which are registered to the bank. In such scenario when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input.

IV. PROPOSEDMETHODOLOGY

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing using visual cryptography. It prevents password and other confidential information from the phishing websites.

The proposed approach can be divided into two phases:

- **Registration phase**
- **Login phase**

1. Registration phase

In the registration phase, user selects a random image. Then using cryptography convert the image into shares on the client side. Send one share to the server for future use and other remains with the user. User can change the share stored on server at any time in case he feels the share is compromised. The trusted server stores unique shares for every user.

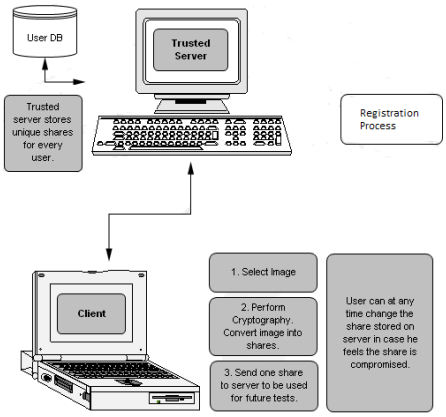

Figure 2: Registration Phase

2. Login phase

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id). Create random public key and private key on the client side using cryptography .Then send the key to trusted server. Using public key encrypt the share2 on the server side. If it is a trusted server then the public key and the encrypted share2 is send to server under test. Server under test send the encrypted share back to the user (may send original or his own share) .Then at client-side it is decrypted using private key. The user's share and the share received from the server under test are stacked together to produce the image. If image obtained is original then the server under test is verified secure or the website is not phishing else it is a phishing site.

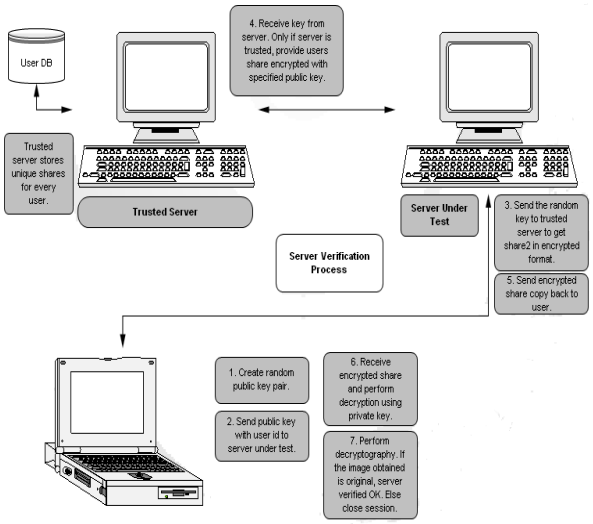

Figure 3: Login Phase

V. IMPLEMENTATION & ANALYSIS

The proposed methodology is implemented using J2EE (Servlets as a Server side technology). Figure 5 shows the result of creation and stacking of shares.

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.

In previous research of Anti-phishing technique [2], as captcha is generated on server side, client can't change it, in order to provide security. However, in mentioned approach it is possible for client to change image when needed. Also RSA public crypto-system is more secure.

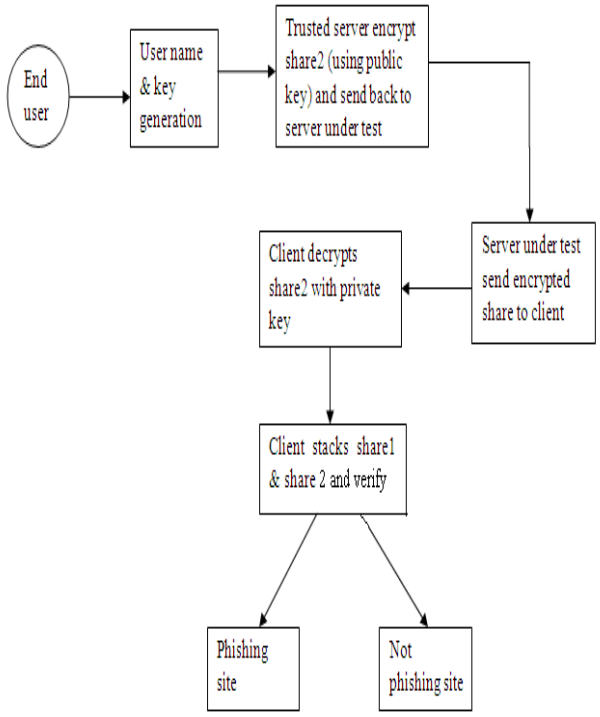

Figure 4: When user attempts to log in into site

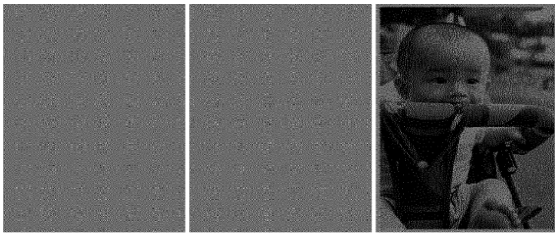

Figure 5:
Share 1 Share 2 Original image

VI. CONCLUSION

As implementation is done using RSA, decryption is not possible without private key. Also as keys are randomly generated, it is not possible for phishing site to get original share. Also if client feels the share is hacked, he can change image so that new shares will be generated. Thus this approach can be used in any online transaction, it is secure and provides authentication.

REFERENCES

[1] Ollmann G., the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[2] Divya James, Mintu Philip, A Novel Anti Phishing framework based on Visual Cryptography, in Proceedings of IEEE International Conference on Information Technology, 2012.

[3] M. Naor and A. Shamir, Visual cryptography, in Proc. EUROCRYPT, 1994, pp. 1–12.

[4] B. Borchert, .Segment Based Visual Cryptography, WSI Press, Germany, 2007.

[5] 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.

[6] 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.

[7] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes, in Journal on Cryptography, vol. 12, 1999, pp. 261-289.

[8] P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with

specifed Whiteness Levels of Reconstructed Pixels, Designs, Codes,
Cryptography, vol. 25, no. 1, 2002, pp. 15-61.

[9] 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.

[10] Ching-Nung Yang, Senior Member, IEEE, Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn, "k Out of n Region Incrementing Scheme in Visual Cryptography", vol. 22, no. 5 MAY 2012

[11] Pei-Ling Chiu and Kai-Hui Lee, A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes, IEEE, 2011.

[12] R.L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.