International Journal of Computer Science and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 4, Sep 2013, 151-156

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

STUDY OF VARIOUS ANTI-PHISHING APPROACHES AND INTRODUCING AN IMPROVED METHOD FOR DETECTING PHISHING WEBSITES

ULKA M. BANSODE[1] & GAURI R. RAO[2]

[1]Department of Computer Engineering, Bharati Vidyapeeth Deemed University, College of Engineering, Pune, Maharashtra, India

[2]Associate Professor, Department of Computer Engineering, Bharati Vidyapeeth Deemed University, College of Engineering, Pune, Maharashtra, India

ABSTRACT

Phishing is an act or fraudulent activity performed by an individual or group to steal or thieve sensitive information of users such as passwords, credit card numbers for malicious purposes, identity theft and financial gain. With the widespread use of Internet most of the people are using online commerce, they are aware of phishing attacks but unaware of how to detect and avoid phishing attacks. Here we have discussed various approaches that are used to avoid phishing attacks. In this paper we have proposed a new method that can be used to detect and prevent phishing attacks. The proposed method makes use of visual cryptography.

KEYWORDS: Image Shares, Phishing, Security, Visual Cryptography

INTRODUCTION

Background

Now a day's online transactions are very common and there are various attacks present behind this. Because of the convenience online transactions are very popular among consumers.

Phishing is a form of online identity theft or it is a type of Internet fraud that aims to acquire personal information of user like credit card information, password, bank account details and other confidential information.

Most of the people are using online transactions but they are unaware of detection and avoidance of phishing attacks so there is increase in these types of attacks which includes online financial fraud.

Because of this phishing has negative impact on economy through financial losses experienced by consumers and businesses and also it results in decreasing consumer confidence in online commerce/transactions.

Banks, e-auctions and e-payment systems are major targets for phishers.

Existing Solution

There are various anti-phishing approaches which can be used to detect and avoid phishing attacks.

"Automated Challenge Response Method" is an authentication mechanism which ensures two way authentications and prevent man in middle attack.

The "DNS Based Anti-phishing" approach includes similarity assessment, blacklist and heuristic detection. Some of the browsers like 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.

Another anti-phishing approach is "A Novel Anti-phishing Framework Based on Visual Cryptography", where image based authentication is performed using Visual Cryptography. The Visual Cryptography is used to preserve privacy of image captcha by decomposing it into two shares and storing these two shares in separate database servers. When both these shares are available simultaneously original image captcha is revealed which can then be used as a password.

RELATED WORK

Phishing web pages are created by malicious people and are forged web pages, designed to mimic web pages of real web sites. Most of these kinds of web pages have visual similarity, those pages look exactly like real web pages. Victims of phishing web pages may expose their important information like bank account number, passwords, credit card number to the phishing web page owners. Phishing includes techniques like instantiation of key loggers and screen captures, man in middle attack, email and spam messages.

Automated Challenge Response Method [1] 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.

Heuristic based anti-phishing technique estimates whether the page has some phishing heuristic characteristics.[2] For example spoof guard toolbar include heuristic characteristics like checking against previously seen images, host name and checking URL for common spoofing techniques.

A Novel Anti-phishing Framework Based on Visual Cryptography [3] is a new methodology for prevention and detection of phishing websites. This approach is divided into 2 phases: Registration and login phase.

In Registration phase, a key string or password is asked from the user. Key string can be combination of alphabets and numbers. In this phase, server randomly generates a string which is concatenated with user provided string to generate image captcha. This image captcha is decomposed into 2 shares. In Login phase, user is asked to enter user-id and then he has to enter his share. Now this share is send to the server, where the user's share and the share stored in the server is stacked together to generate image captcha. The user has to enter the text displayed in image captcha which can serve as a password to login into the website.

The DNS Based Anti-phishing approach [4] 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.

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.

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

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

ISSUES AND CHALLENGES

- Blacklist based technique cannot detect the websites that are not in blacklist database.
- Accuracy is not enough if Heuristic based techniques are used, because an attacker can use technical means to avoid detection of heuristic characteristics.
- In case of techniques based on similarity assessment, it requires too long time to calculate pair of pages. Low accuracy rate because, this method depends on many factors such as text, images and similarity measurement techniques.

VISUAL CRYPTOGRAPHY

Visual cryptography is a secure method that encrypts an image by breaking it into shares. It is the art of sending and receiving encrypted messages that can be decrypted only by sender or receiver.

Visual cryptography can be achieved by following access structure schemes:

- (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.
- (n , n) Threshold VCS scheme - This scheme encrypts the secret image to n shares such that when all n of the shares are combined, secret image will be revealed.
- (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.

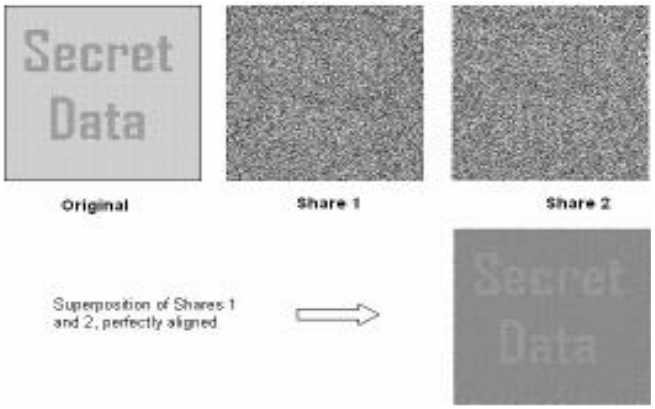

Figure 1: Example of (2, 2) Visual Cryptography Scheme

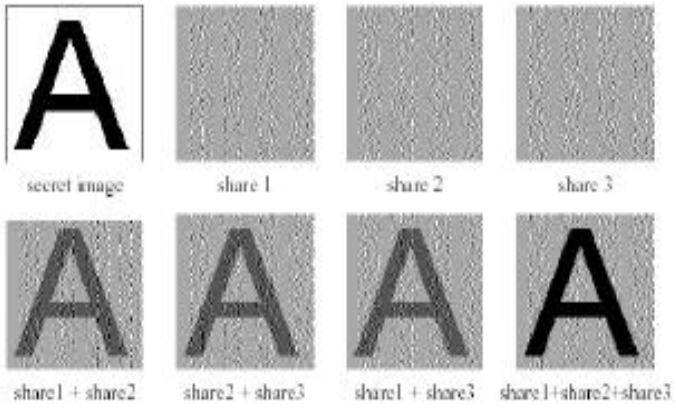

Figure 2: Example of (2, 3) Visual Cryptography Scheme

CURRENT METHODOLOGY

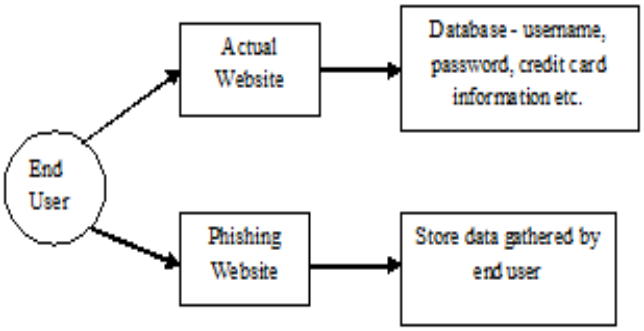

Figure 3: Current Scenario

The figure 3 shows the current scenario. When user accesses his information online by logging into his bank account or secure mail account, the person enters information like username, password, and credit card information etc. on the login page. But this information can be captured by attackers using various phishing techniques. (For instance Phishing website can collect the login information the user enters and redirect him to the original site.)

PROPOSED METHODOLOGY

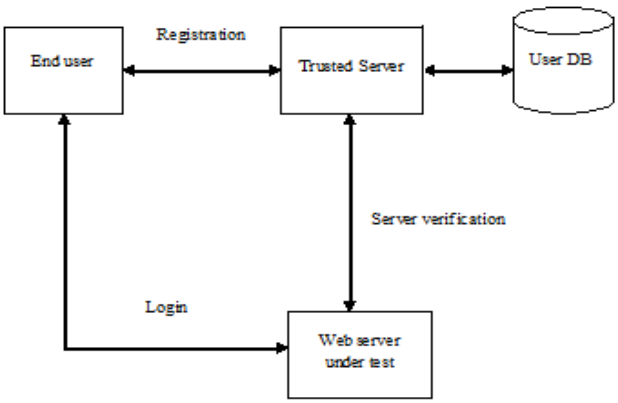

Figure 4: Proposed Methodology

Figure 4 represents a proposed methodology. When user registers with the server, server generates pair of unique keys for the user. From that pair one key for the user is saved on the user database of the trusted server and another key is propagated to the user.

When the user logs into the system through the web server1, user selects a random image which is available on his/her machine (Every time when user logs into the system he/she can select any image available onto the system).

This image is divided into two shares such that one share is kept with the user and other share is encrypted and sent to the web serevr1. Web server1 sends this encrypted share along with its details to the trusted server. Trusted server provides decrypted version of this share if and only if server1 was registered with trusted server. The decrypted share is sent back to the client. At the client side decryptography is performed to obtain the original image by stacking together the shares.

If the original image obtained is as is, the website is genuine/secure website and not a phishing website.

CONCLUSIONS

With the widespread use of the Internet security issue has become a top priority. This paper reviewed the various anti-phishing approaches. Also this paper highlights the challenges and limitations involved with these approaches. In this

paper we have proposed a new approach for detection and prevention against phishing attacks. This approach is based on Visual Cryptography. With the help of VC the security of the online banking system will be increased to some extent.

REFERENCES

1. Thiyagarajan, P.; Aghila, G.; Venkatesan, V.P.; "Anti-Phishing Technique using Automated Challenge Response Method'", in Proceedings of IEEE- International Conference on Communications and Computational Intelligence, 2010.
2. Ishtiaq, S.; Nourian, A.; Maheswaran, M.;" CASTLE: A social framework for collaborative antiphishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2009.
3. Mintu Philip;Divya James;" A Novel Anti phishing Framework based on Visual Cryptography" in International Journal of Distributed and Parallel Systems, Vol. 3, No. 1, January 2012.
4. Liang Xiaoying.; Sun Bin.; Wen Qiaoyan.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE-Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.
5. M. Naor and A. Shamir; "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
6. B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.
7. D. Jin, M. S. Kanakanahalli and W-Q Yan; .Visual Cryptography for Print and Scan Applications, IEEE Transactions, ISCAS-2004, pp. 572-575.