INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3046 – 3051
RECEIVED : 28.02.2018 PUBLISHED : 29.03.2018
March 29, 2018

ANTI-PHISHING BASED BANKING APPLICATION USING IMAGE AUTHENTICATION

Mrs.A.Ezhilarasi.,M.Sc (computer science) II[cd] year.
(Guide) Asst Prof.S.Lalitha.,M.Phil.,M.Tech.,
Department of Computer Science, Kamban Arts And Science College for Women, Thiruvannamalai.

ABSTRACT

Phishing is an attempt by an individual or a group to thieve 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 user have proposed a new approach named as "A Novel Antiphishing framework based on visual cryptography" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (vc) is used. The use of visual cryptography is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password.

1. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks here after this. In this type of different attack, phishing is known as a foremost protection threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so efficient. Thus the safety in these cases be awfully high and should not be easily tractable with execution acceptance. Nowadays, the majority of the application is only as protected as their primary system. Since the propose and expertise of middleware has enhanced gradually, their detection is a complex problem. As a result, it is nearly not possible to be sure whether a processor that is linked to the internet can be considered trustworthy and secure or not. Phishing scam is also becoming a hitch for online banking and e-commerce users. The query is how to hold applications that require a high point of security. Phishing is a form of online individuality stealing that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication.

One definition of phishing is specified as “it is a illegal activity using social engineering techniques. Phishers try to falsely acquire susceptible information, such as passwords and credit card details, by hidden as a trustworthy person or business in an electronic communication”. Another complete definition of phishing, states that it is “the act of transfer an email to a user falsely claim to be an establish legal enterprise into an attempt to scam the user into yielding personal information that will be used for self theft”. The conduct of identity theft with this acquire receptive information has also

become easier with the use of technology and identity theft can be describe as "a crime in which the fake obtains key pieces of information such as Social Security and driver's license information and uses them for his or her own grow". Phishing [1] attacks rely upon a combine of technological deception and social engineering practices.

2. STUDY OF EXISTING SYSTEM

Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of real web sites. Most of these kinds of web pages have high visual similarities to scam their victims. Some of these kinds of web pages look exactly like the real ones. Victims of phishing web pages may expose their bank account, password, credit card number, or other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, installation of key loggers and screen captures.

DISADVANTAGES

Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database. Because the life cycle of phishing websites is too short and the establishment of blacklist has a long lag time, the accuracy of blacklist is not too high. Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to use technical means to avoid the heuristic characteristics detection. Similarity assessment based technique is time-consuming. It needs too long time to calculate a pair of pages, so using the method to detect phishing websites on the client terminal is not suitable. And there is low accuracy rate for this method depends on many factors, such as the text, images, and similarity measurement technique. However, this technique (in particular).

3. PROPOSED SYSTEM

The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined. VCS 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. 2. (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. 3. (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. In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Figure.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.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3046 – 3051
RECEIVED : 28.02.2018 PUBLISHED : 29.03.2018
March 29, 2018

ADVANTAGES

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

4. IMPLEMENTATION

Login: In the Login phase first the user is prompted for the username (user id).Then the user is asked 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. The image captcha is displayed to the user. Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.
View Users
View Transactions

User:

- User
- Register
- Register our personal details and account details
- Upload our authentication image.
- Send user’s mail share 1 image
- Registration completed
- Login
- Login Process 1 (User enter username and password)
- Process 2 (Upload authentication image from user mail)
- Login successfully completed.
- View Profile

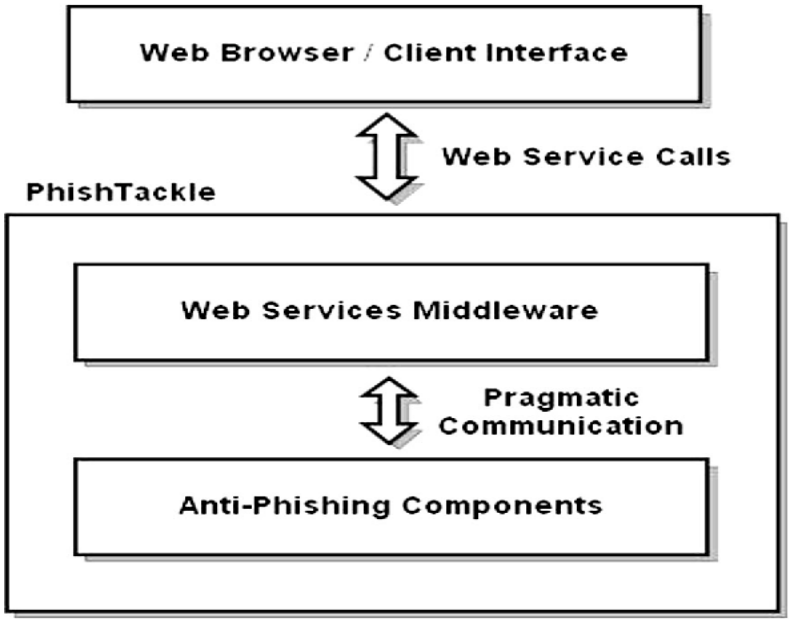
Register: Split the original images in 2 equal parts call in share1 and share2. First share1 images store in local system. The second share2 images store in server site database. we propose a new algorithm to encrypt binary images. The proposed scheme is described in several steps. In the first step, we present a new basis to reduce the amount of data required to present the image. In the second step, the image is split into d blocks, which is used in new images of the same size as the original one, and represent them in the new basis to obtain a key-image and encrypted images. The parameters obtained by this transformation are considered as key-image for the encryption and decryption algorithm. The decryption algorithm is performed by the subtraction between each encrypted image and key-image,

then summing them in an image to obtain the original one. In the same way, we can apply our proposed algorithm to encrypt a database of binary images. Experimental results demonstrate the efficiency of the proposed approach.

Login: A binary image (bi-valued image) is the type of simple image that is widely used in various electronic applications such as fingerprint analysis, robot vision, motion detection and character recognition. It often appears as cartoons in newspapers and magazines. Moreover, binary images frequen emerge as the result of many automatic tasks, such as binarisation, halftoning, edge detection, segmentation, and thresholding. Certain input/output devices and sensors, like for examples laser printers, fax machines.

Compare original Images: Among the most published works, we can find in [16] a scan language is proposed by Bourbaki in 1986 as a language for efficient accessing of a two dimensional array. In [17] a parallel implementation version for the scan language is presented, which shows that the parallel expansion scheme is faster and requires less storage space.

5. SYSTEM ARCHITECTURE



AES ALGORITHM

- AES decryption is not identical to encryption since steps done in reverse.
- but can define an equivalent inverse cipher with steps as for encryption
- but using inverses of each step with a different key schedule.
- works since result is unchanged when
- swap byte substitution & shift rows
- swap mix columns & add (tweaked) round key.

- clear a replacement for DES was needed have theoretical attacks that can break it have demonstrated exhaustive key search attacks can use Triple-DES – but slow, has small blocks US NIST issued call for ciphers in 1997 15 candidates accepted in Jun 98 5 were shortlisted in Aug-99 Rijndael was selected as the AES in Oct-2000 issued as FIPS PUB 197 standard in Nov-2001.
- As a solution to this problem, in this paper, we present an extensive study of enhancing the throughput of AES encryption algorithm by utilizing the state of the art multicore architectures.

We take a sequential program that implements the AES algorithm and convert the same to run on multicore architectures with minimum effort. We implement two different parallel programmes, one with the fork system call in Linux and the other with the pthreads, the POSIX standard for threads. Later, we ran both the versions of the parallel programs on different multicore architectures and compared and analysed the throughputs between the implementations and among different architectures. The pthreads implementation outperformed in all the experiments we conducted and the best throughput obtained is around 7Gbps on a 32-core processor (the largest number of cores we had) with the pthreads implementation.

6. CONCLUSION

Phishing attacks are very common in day-to-day life because it is done globally and very easily it can store the user's confidential information. This data can be used by attackers. Phishing websites as well as human users can be easily identified using our proposed "An Anti-phishing framework based on Visual Cryptography".

The proposed methodology protects confidential information of users using 3 layers of security. The proposed methodology can be used to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market etc.

7. FUTURE RESEARCH WORK

Netcraft's phishing site feed is consistently recognized in third party reviews as the most effective blocking mechanism for protecting customers against phishing, and is licensed by leading browsers, anti-virus and content filtering products, firewall and network appliance vendors, mail providers, registers, hosting companies and ISPs.

Future Research work includes how to effectively correlate connections was prepared by,

- Extensive Automation and Preparation
- Hosting Company and Register Intraction
- Upstream Bandwidth Providers
- Local Law Enforcement Agency
- Transparent Progress Reporting

8. REFRENCES

1. Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.
2. [3].- Ren-Junn Hwang,"A digital image copyright protection scheme based on visual cryptography", Tamkang Journal of science and engineering, Vol.3, No. 2, pp. 97-106(2000).
3. [4]. Divya James, Mintu Philip, "A novel Anti-phishing framework based on visual cryptography", IEEE 2012.
4. [5]. M.Naor and A.Shamir,"Visual cryptography", in Proc. EUROCRYPT, 1994, pp.1-12. IJDPS Vol.3, No.1, 2012.