International Journal of Electrical and Computer Engineering (IJECE)
Vol. 5, No. 6, December 2015, pp. 1511~1515
ISSN: 2088-8708

Anti-Phishing Techniques in Cryptography

Akshey Nanda, Himanshu Gupta
Amity Institute of Information Technology, Amity University Campus, Sector-125, Noida (Uttar Pradesh), India

Article Info

Article history:

Received Jun 30, 2015
Revised Aug 26, 2015
Accepted Sep 15, 2015

Keyword:

Finger print
OTP
Phishing
Visual Cryptography

ABSTRACT

Phishing is a process in which Phishers try to leak out the credentials of users by hosting a fake web page on user's browser. To save users from phishing attacks, many researchers have dug deep and presented their insights. Nowadays, in the era of 21st century, banks are using the OTP and visual cryptography for the authentication of both sides i.e. user and the bank. In this paper, we are proposing a methodology in which a user will need to give his finger prints as an authentication.

Corresponding Author:

Akshey Nanda,
Amity Institute of Information Technology,
Amity University Campus,
Sector-125, Noida (Uttar Pradesh), India.
Email:

1. INTRODUCTION

Nowadays online transactions have become very common. Most of the users use the medium of online transaction rather than cash as it's actually easy for not keeping cash handy. Also, one doesn't have to go to the bank. Indeed, online transactions have made life easier and stress-free. But the contradiction is, this technology has given a clean chance to Phishers to leak your credentials. The way they leak the credentials of a user is known as phishing technique. In this, the Phisher hosts his own web page and that is where you enter your user name and password and send it to the Phisher [2], [10]. According to your view of knowledge, you have sent your request to the server but actually it is sent to the Phisher because the hosted page belonged to Phisher and not to server. So this is how, a Phisher leaks your credentials and misuses them. A large no. of researchers have given their ideas to reduce phishing like visual cryptography and the OTP etc. but these techniques have not been able to completely demolish the phishing technique. Although, the number has reduced but not vanished yet. [3]-[7]. In this research, we have proposed a way in which one can combine biometric of finger prints and OTP for authentication of user and server.

1.1. Visual Cryptography

Visual cryptography is a technique used for user and server authentication. This technique was proposed by Naor and Shamir [1]. In this technique, they proposed the fact that if the system generates a random image and divides that image in two or more shares if we concatenate these two shares. The image created by concatenating these two images will be then matched with original image [5], [8]. And if the images are matched, then both sides imply authentication else there is some Phisher in between. We can divide the image in many shares as shown below:

1) (2, 2), Threshold VCS scheme: This is the simplest threshold scheme that takes a secret message and encrypts it in two different shares which further reveal the secret image when they are concatenated.

2) (n, n), Threshold VCS scheme: This scheme encrypts the secret image to n shares in such a way that when all n of the shares are concatenated, the secret image will be revealed.

3) (k, n), Threshold VCS scheme: This scheme encrypts the secret image to n shares in such a way that when any group of at least k shares is overlaid, the secret image will be revealed.

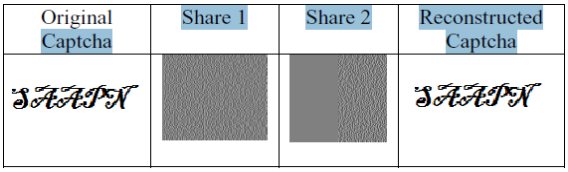

Figure 1. Visual Cryptography

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. In Figure.1, Share 1 denotes the shares of white pixel and Share 2 of 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). None of the shares provide any clue about the original pixel as different pixels in the secret image are encrypted using independent random choices.

In Figure 2, 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.

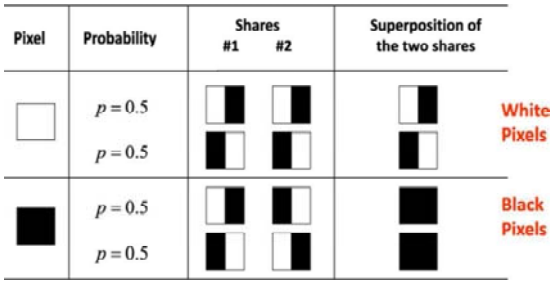

Figure 2. Showing pixels in visual cryptography

1.2. Biometric Security: Finger Print Processing

As scientists have proved that some features or attributes of a person define his uniqueness. These features are one in a billion. Similarly, in biometric feature, we can take the Retina, iris and finger prints which apparently are unique for every individual. This is why nowadays companies have started using biometric for attendance [9].

And as a result, this has brought transparency in the system because a person can mark only his attendance. No other person can mark the attendance of some other individual because by nature's law, nobody can steal the finger prints of any person.

In Figure 4, it is shown that how our system works to check the fingerprints of a person.

Figure 3. Finger print

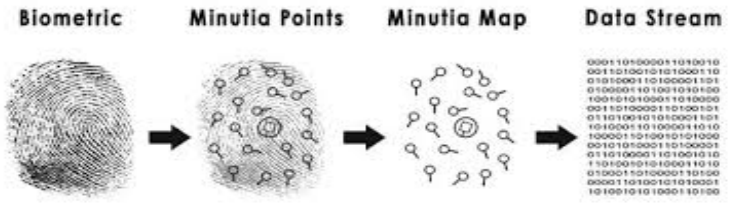

Figure 4. Finger Print Processing

1.3. Background

As per the current methodology, for pursuing an online transaction, a user visits the website of the bank and then submits his username and password to the server. Server authenticates the username and password. If they are authenticated then the user will be logged in and will have the access of his account. Also, if a user wants to perform any transaction, he has to complete the process of OTP. In this methodology, if Phishers host their own web page, then they will be able to leak the usernames and passwords easily [4].

2. RESEARCH METHOD

We are proposing a way to increase the security for online transactions to reduce the phishing attacks. In this proposed way, a user will provide the bank with his finger prints. Whenever the user wants to do any transaction, he will visit to the bank's URL and enter his username and password. If username and password are authenticated by the bank, then the bank will further ask for the OTP sent on his phone. After the OTP authentication, the user will be logged in his account. Not only this, but also if the user wants to perform any changes in his account for illustration, change of password, he'll again have to give his finger prints for the authentication. These finger prints will be divided in two parts with different values. One share will be discarded and the other share will be sent to the bank. The bank will also divide the finger prints with same value and discard the different image that was received from the user's end. Then, the bank will concatenate these two images and match them with the finger prints given by the user at the time of registration. After these two images are matched, the user will be authenticated and hence, transaction will be proceeded. But before the finger print process, the user will also have to go for the OTP process for authentication.

There will be two phases in the online transaction:

1) Login

2) Online Payment

1) Login

In the login phase, the user will first enter the username and password and then will submit it to the Bank's server. Then the bank's server will send the OTP on the user's phone through message. The user will enter the OTP received on his phone. The bank will authorise it. And after the OTP's authorisation done by the bank, the user will get the access to his account.

2) Online Payment

After the login phase, the user will get the access to his account. Now the user can only check his balance and if he wants to perform any transaction or do any changes in his account, he'll have to provide his finger print authentication. Even if the user wants to change the password, he has to take the finger print authentication. Ultimately, these two phases will bring more security than the current methodology because even if the Phisher gets the username and password, then also he will not be able to take the access of the account because of the OTP.

The complete process of biometric authentication is shown below in Figure 5.

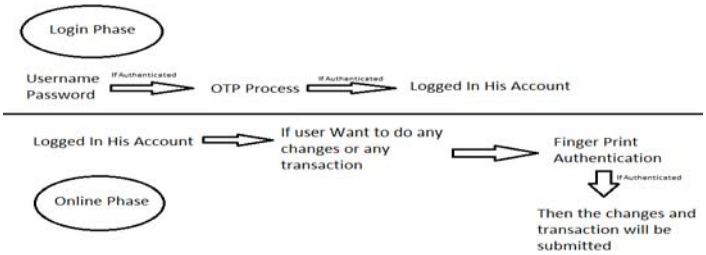

Figure 5. Biometric Authentication

2.2. Matching Patterns in Fingerprint

When user will give his finger prints for the authorization purpose, his finger prints will be divided into two shares. One will have some pixels and other will have some pixels. One of the shares will be transmitted to the bank for the authorization. The bank will also divide the image of finger prints of the same user with the same algorithm. Also, the bank will have the same two shares of the finger prints. The bank will concatenate these two shares (one received from the user's end and the other which is done by the bank). If the image generated from concatenation of these two shares match the original finger prints, then the user will be authenticated, as shown in Figure 6.

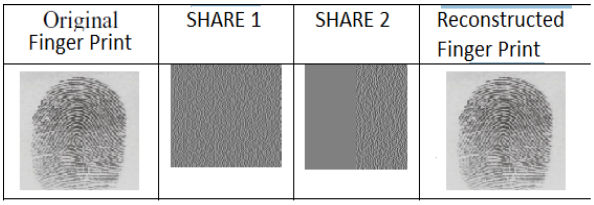

Figure 6. Shares of finger print

Now the question arises, by which value the image will be divided into shares. We have to use the value which will be known to the bank and the user only. Not any third person should be aware of this value. For this, we will use the OTP value that was entered by the user in login phase. The bank had sent the OTP on the user's phone in the login phase. The application which will divide the finger prints in two shares will remember the OTP entered by the user. If the user wants to do any transaction or any change in the account, he will give his finger prints for authentication. The application that will divide the finger prints in two shares will generate the value from the OTP and the algorithm will use these values for dividing the finger prints in two shares. The bank will also know the OTP sent and will use the same value for finger print shares. The OTP will not be known to the phisher. So he will not be able to use finger prints even if he gets the copy of that.

3. CONCLUSION

In the current methodology, the user enters the username and the password and gets the login in his account. And if the user has to perform any transaction, he has to go for OTP, so in this case if the Phisher is hosting his own website, then the user's username and password will be subsequently leaked . And thus, the Phisher will easily get the access of his account. In our methodology, the user will enter the username and password, then he will get the OTP on his phone to enter on the website. After this, if user wants to do any transaction or any changes, he further has to give his finger prints for authentication. And the way finger prints are divided into two shares is highly secure.

4. FUTURE WORKS

Previously, the user first had to authorise through his username and password. Then if the user wanted to do any transaction, he had to go through the OTP process. In our methodology, we have proposed a way in which the user will be first authenticated by his user name and password and then will receive an OTP. Gradually, the user will then have to go through the OTP process because only then, he will get the access of his account. For any transaction, the user has to do the finger prints process. In future work, we will go for the practical implementation of this methodology and also for some new research paper on the same topic of making online transactions more secured. Because for phishing attacks, the phishers have to get all the necessary elements such as username and password, OTP, finger prints, value used for dividing the finger prints etc. and indeed, it will be difficult to attain these things. So, using this methodology the online transaction will become more secured.

REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography," *in the proceeding of EUROCRYPT*, pp. 1-12, 1994.
[2] Divya James Mintu Philip "A Novel Anti Phishing framework based on Visual Cryptography", *in IEEE transaction*, 2012,

[3] Ahmad Alamgir Khan, "Preventing Phishing Attacks using One Time Password and User Machine Identification", *in International Journal of Computer Applications*, Vol. 68, No. 3, pp 7-11, 2013.
[4] Gaurav, Madhuresh Mishra, Anurag Jain, "Anti-Phishing Techniques: A Review", *in International Journal of Engineering Research andApplications (IJERA)*, pp. 350-355, 2012.
[5] Mrs. A. Vinodhini, M. Premanand, M. Natarajan, "Visual Cryptography Using Two Factor Biometric System for Trust worthy Authentication", *in International Journal of Scientific and Research Publications,* Vol. 2, No. 3, pp 1-5, 2012.
[6] Jyoti Chhikara, Ritu Dahiya, Neha Garg, and Monika Rani, "Phishing & Anti-Phishing Techniques: Case Study", *in International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. 3, No. 5, pp. 458-465, 2013.
[7] Bhushan Yenurkar1, Shrikant Zade, "An Anti-phishing Framework with New Validation Scheme using Visual Cryptography", *In International Journal of Computer Science and Mobile Computing,* Vol. 3, No. 2, pp. 739-744, 2014.
[8] Gaurav Palande, ShekharJadhav, Ashutosh Malwade, Vishal Divekar, and Prof. S. Baj. "An Enhanced Anti-Phishing Framework Based on Visual Cryptography", *International Journal of Emerging Research in Management & Technology,* Vol. 3, No. 3, pp 43-46, 2014.
[9] V. Krishna Chaitanya Reddy, B. Sukumar, S. Javeed Hussain, "ARM 9 Based Intelligent System for Biometric Figure Authentication", *TELKOMNIKA Indonesian Journal of Electrical Engineering*, Vol. 13, No. 2, pp. 209-214, 2015.
[10] Yunsang Oh, Takashi Obi, "Identifying Phishing Threats in Government Web Services", *International Journal of Information & Network Security (IJINS)*, Vol. 2, No. 1, pp. 32-42, 2013.

BIOGRAPHIES OF AUTHORS

Akshey Nanda is a Post-Graduate student of Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India. He is pursuing M.Sc. in Network Technology and Management and also have a certification of CCNA Routing and Switching.

Dr. Himanshu Gupta is associated with academics and research activities since last ten years. He is working as a Senior Faculty Member in Amity Institute of Information Technology, Amity University, Noida.
Dr. Himanshu Gupta is having specialization in Network Security & Cryptography. He is having prestigious membership in various reputed International Technical and Research Organizations as IEEE Computer Society (USA), TIFR (India), CSI (India), CSTA (USA), IACSIT (Singapore), CRSI (India), UACEE (Australia) and World Association of Young Scientists (Paris). He has successfully completed a patent titled as "A Technique & Device for Multiphase Encryption" under the domain area of Network Security & Cryptography in the field of Information Technology and many more patents have been filed in same domain.
Dr. Himanshu Gupta has attended many National and International Conferences, Seminars and Workshops and presented many research papers in the field of Information Technology. He has visited to Malaysia, Singapore, Thailand, Cambodia, Vietnam and Indonesia for his academic and research work. He has delivered many technical sessions on ―Network Security & Cryptography‖ in the field of Information Technology in various reputed International Conferences, World Summit and other foreign universities as an Invited Speaker. He has many Research Papers and Articles in the field of Information Technology, which have been published in various reputed Conference Proceedings and Journals.