ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Survey on an Advanced Technique for Anti-Phishing Using QR-Code & Visual Cryptography

Rupesh Mahajan, Ramabhishek, Vaibhav Bakshi, Harsh Raj, Prasad Kulkarni

Professor, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

Student, Dept. of I.T., D.Y.P.I.E.T., Pimpri, Pune, India

ABSTRACT: Phishing is an attempt to gather sensitive information such as usernames, passwords, credit card credentials or some other sensitive information from the end user and misusing it for cybercrimes. Therefore, the main aim is to develop real time system which will detect and prevent Phishing using QR code & Visual Cryptography. In this paper we have proposed a new technique "An Advanced technique for Anti-Phishing Using QR-code & Visual cryptography" to prevent such phishing attacks and protect networks. In this approach an image based authentication is used in which the original image is converted into QR code and then partitioned into two halves which are stored in separate databases. This division is achieved with the help of Visual Cryptographic algorithms. The end user combines these shares to generate an OTP which provides better security over the transaction. The original image cannot be obtained without combining the individual parts. Once the original image captcha is revealed to the user it can be used as the password .This approach uses two server authentication and image processing which provides better security during online transactions.

KEYWORDS: Anti-Phishing, Visual Cryptography, Image Captcha, QR codes.

I. INTRODUCTION

Online transactions are nowadays become very popular, due to this security over the network has become an important issue. As far as the security and cyber-attacks are concerned, phishing is identified as a major security threat and new innovative ideas are being implemented with this in each second so preventive mechanisms should also be so effective .Thus the security in such cases is at highest priority. So here we introduce a new and secure technique which can be used to detect and prevent phishing attacks which is named as "An Advanced technique for Anti-Phishing Using QR-code & Visual cryptography". In this method, a system capable of identifying fake servers and preventing the misuse of sensitive user credentials is developed which allows users to differentiate between legitimate and phishing websites. So, by knowing this he can securely perform his further proceedings or transactions. Here the OTP is converted into QR code (Quick Response) and divided into two shares. Here, we used the concept of an improved visual cryptography. Visual Cryptography (VC) is used here to divide the image into shares, encryption and in order to reveal the original image appropriate numbers of share should be combined. So the end user gets these shares and decrypts them to get the OTP which is used for further transaction. Due to the use of various techniques and algorithms this approach enables a highly secure environment for online transactions.

II. RELATED WORK

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 greater visual similarities to scam the user. Some of these kinds of web pages

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

look exactly like the real ones. Victims of phishing web pages may reveal their bank account details, credit card details, or other important information to the phishing web pages. It includes techniques such as gaining important information from users through email and spam messages, man in the middle attacks, and installation of key loggers. In the current situation, when the end user wants to access his confidential information online (for money transfer or payment gateway) by logging into his bank account or online payment gateway, the person enters information like username, credit card no, password 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 entered by user and redirect him to the original site).In existing system, there is no mechanism through which the end user can authenticate the server.

1. CURRENT 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 greater visual similarities to scam the user. Some of these kinds of web pages look exactly like the real ones. Victims of phishing web pages may reveal their bank account details, credit card details, or other important information to the phishing web pages. It includes techniques such as gaining important information from users through email and spam messages, man in the middle attacks, and installation of key loggers. In the current situation, when the end user wants to access his confidential information online (for money transfer or payment gateway) by logging into his bank account or online payment gateway, the person enters information like username, credit card no, password 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 entered by user and redirect him to the original site).In existing system, there is no mechanism through which the end user can authenticate the server.

2. PROPOSED SYSTEM

In this proposed system, the OTP is converted into QR code and divided in shares which distributed to end user and merchant server. The end user combines these shares to get OTP. If the merchant server is fake then the false OTP will be obtained which will block further proceedings. In this way end user can authenticates merchant server which was not provided in current scenario. Since the Bank server and end user both authenticate merchant server, this architecture provides two-server authentication system for high security.

3. VISUAL CRYPTOGRAPHY

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. It's an image based technique which protects the data in image form. They demonstrated a visual secret sharing scheme, where an image was partitioned into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares did not reveal any information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

4. QR CODE

QR code(Quick Response Code)consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging devices and processed until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image. As it consists of square dots and blurred form of images, it is very difficult to decode it.

III. ARCHITECTURE

The architecture of the proposed system consists of following components:

1. Bank Server.
2. Merchant Server.
3. Client or End User.

1. BANK SERVER

The Bank server has following functionalities:

1) to store the details of all merchant servers.
2) To authenticate Merchant server & end user.
3) To generate OTP & apply visual cryptography.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

2. **MERCHANT SERVER**

A merchant server is an intermediate server which accepts requests from end user and communicates with bank server. The merchant server accepts the share of an OTP from Bank sever and sends to end user for authentication.

3. **CLIENT OR END USER**

Client is the person who is performing the online transactions. It requests merchant server for any transaction and gets response. Client provides its credentials and waits for the OTP from Bank server. It combines the shares from Bank server and Merchant server to get original OTP for further processing.

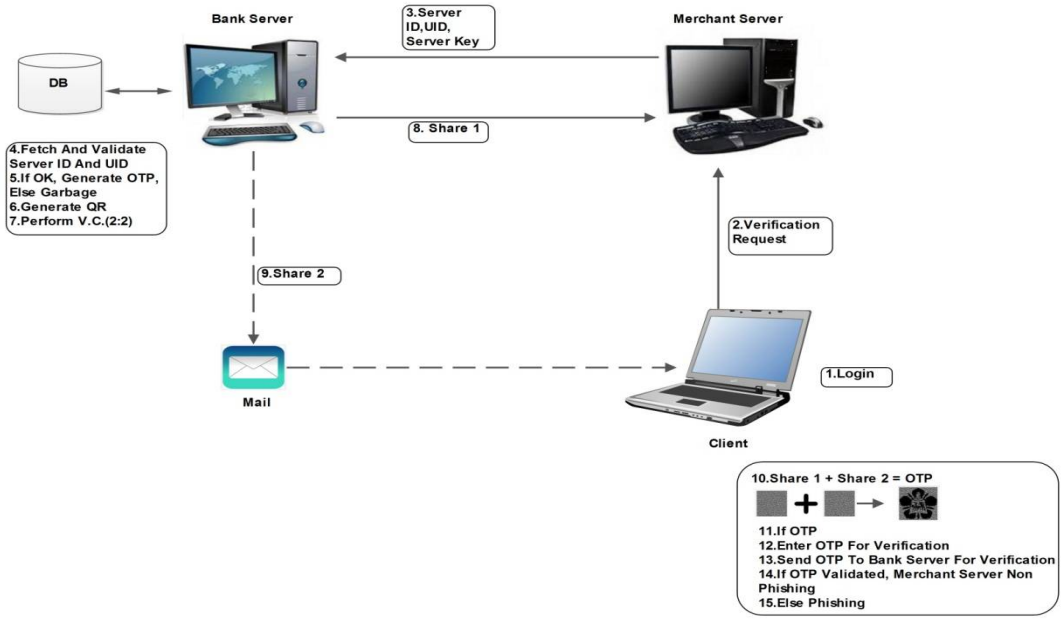

Fig.1: Anti-Phishing using QR code & visual cryptography Architecture.

IV. PROPOSED METHODOLOGY

Our proposed system will be able to detect and prevent the phishing attacks against illegal online transactions. Our methodology is based on the Anti-Phishing Image processing scheme using visual cryptography. It prevents password and other confidential information from the phishing attacks.

V. ACKNOWLEDGEMENT

We would like to thank and express our heartfelt gratitude to our guide Prof. RUPESH MAHAJAN, DYPIET for his expert guidance and encouragement.

VI. CONCLUSION AND FUTURE WORK

Due to the vast use of internet and transfer of large amount of private data, security over the network has become an important issue. This information is used by the attackers which are indirectly involved in the phishing process. Any illegal activity in relation with phishing done by the attackers can be easily identified using our proposed methodology "An Advanced technique for Anti-Phishing Using QR-code & Visual cryptography". Our proposed technique provides more security as a random image is chosen for a particular session and it is converted in QR code and divided into two

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

shares using Visual Cryptography. As image processing is involved, it is more secure system than the current systems. Hence it provides much better securitistic algorithm and protects the personal information data entered by the user. This system provides two-server authentication and due to use of QR code and Visual Cryptography, the system becomes less vulnerable against the cyber-attacks.

REFERENCES

1. QingxiangFeng.; Kuo-Kun Tseng.; Jeng-Shyang Pan.; Peng Cheng and Charles Chen.; "New Antiphishing Method with Two Types of Passwords in OpenID System", in Proceedings of IEEE Fifth International Conference on Genetic and Evolutionary Computing,, pp. 40-47,2011.
2. Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communication and Trusted Computing, , pp. 35-44,2010.
3. G. R. Blakley, .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.
4. Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee," Online Banking Authentication System using Mobile-OTP with QR-code", E-ISBN : 978-89-88678-30-5, Page(s): 644 – 648, Nov. 30 2010-Dec. 2 2010.
5. Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee," Online Banking Authentication System using Mobile-OTP with QR-code", E-ISBN : 978-89-88678-30-5, Page(s): 644 – 648, Nov. 30 2010-Dec. 2 2010,.
6. T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,.in Proceedings of IEEEInternational Conference on Information Technology, pp. 41-43,2007.
7. E. Bresson, O. Chevassut, and D. Pointcheval, "Security Proofs foran Efficient Password-Based Key Exchange," Proc. ACM Conf.Computer and Comm. Security, J. Brainard, A. Juels, B. Kaliski, and M. Szydlo, "A New Two- Server Approach for Authentication with Short Secrets," Proc. USENIX Security Symp.pp. 241-250, 2003.
8. M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks," Advances in Cryptology (Eurocrypt '00), pp. 139-155, 2000.
9. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,.in Proceedings of IEEEInternational Conference on Information Technology, pp. 40-44,2007.