A Novel Anti-Phishing Framework using Visual Cryptography

Sagarika Naik
Student
Information Technology
Atharva College of Engineering
Mumbai, India

T Varsha Dass
Student
Information Technology
Atharva College of Engineering
Mumbai, India

Khushboo Gohil
Student
Information Technology
Atharva College of Engineering
Mumbai, India

Pratik Ghogre
Student
Information Technology
Atharva College of Engineering
Mumbai, India

Reena Somani
Assistant professor
Information Technology
Atharva College of Engineering
Mumbai, India

***Abstract*— Phishing is an attempt by an individual or a group to steal confidential information such as passwords, credit card information. from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Nowadays, phishing attacks are increasing at an alarming rate for e-commerce websites. We aim to provide a novel anti-phishing approach which relies on visual cryptography. According to this novel approach, a user generates two shares of an image using (2, 2) visual cryptography scheme. The client stores the first share of this image and the second share is uploaded at the time of user registration. After this, the proposed system asks for some other information like second share of the image, username, and password. During each login phase, the user, along with identifying as a legitimate user, can verify the legitimacy of a website by getting secret information with the help of stacking both shares. There are many existing approaches based on cryptography but they all suffer from "False Positive" notification. However, proposed approach does not suffer from False Positive (FP) notification and outperforms all existing approaches. Graphical password scheme is an authentication system that works by having the user select images from a set of images, that is presented in a graphical user interface. During registration, the user selects three images from the displayed set of images in a grid view. If the user selects the same images during login process, they can proceed for the pair based session password. If the user fails to select the correct images chosen by him during the registration process the user will be barred and will have to login again with correct images. This approach helps to enhance security.**

Keywords*— *Phishing; Image Captcha; Sharing; Security; Visual Cryptography.

I. INTRODUCTION

Online transactions, nowadays have become very common and with the advent of digital payments, many threats and attacks have also become commonplace. Among various attacks, phishing is identified as a huge threat to security and new innovative ideas are arising to dupe users. So preventive mechanisms should be very effective. Thus the security in these cases is very high and should not be easily tractable with implementation ease.

Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, the detection of phished content is an everyday problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a trouble for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

Phishing is an attempt by an individual or a group to thieve 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 framework known as "A Novel Anti phishing framework based on visual cryptography" to solve the problem of phishing. Here an image based authentication scheme and 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; and the other phase is during the registration, when the users have to select any random images which will be useful for authentication of user when he tries to login later. The individual sheet images do not reveal the identity of the original image captcha.

II. VARIOUS METHODS

A. A Novel Anti-phishing framework on cloud based Visual Cryptography

F

This work by Nagesh Soradge , and K. S.Thakare, carried out in June 2014, presents a novel method which can be used as a secure path in opposition to phishing which is named as "A novel technique against phishing using visual cryptography". In this approach the concerned website crosschecks its own identity and manifests that it is a legitimate website (to use bank transaction, E-commerce and online booking systems etc.) in front of the end users and ensures that both the sides of the system safe and authenticated. In this technique, the notions of image processing and visual cryptography are used. Image processing is a method of feeding in an image and getting the output as either a better form of the original image and/or an image with characteristics of the original image. Visual Cryptography (VC) is a technique of dividing an image into shares, with a requisite such that arranging a sufficient number of shares discloses the secret image.

The proposed method can be divided into two phases, In the registration phase, along with the personal information a password and an image of users' choice is taken from the user. The image obtained from the user is bifurcated into shares. One of the shares is kept on the user's cloud account which is created by server for each particular user. The share which is to be stored on the server is again bifurcated into four shares and stored over the server cloud along with a replica for increasing the availability and security.

In the Login Phase, when a concerned user wants to access his account, the user is asked to enter his username and password. After receiving the strings of username and password, the corresponding share which is stored onto the server cloud is retrieved based on the replica. Eventually the correlated shares are retrieved onto the server from the users cloud account and server cloud. From these two shares, the original users' choice of picture which he had uploaded at the time of registration is formed. Server generates a CAPTCHA image and displays on the login page along with the formed image.

B. Two level Authentication System Based on Pair Based Authentication and Image Selection

This work by Madhuri Achmani, Radhika Dehaley, Anuja Gaonkar, Anindita Khade was carried out in April 2016.It uses Image Selection Authentication Scheme to ensure the two-way authentication scheme. Graphical password scheme is an authentication system that works by making the user select images from a pre-ordained set of images, presented in a graphical user interface. This is a technique that has been evolving in recent years as a safer way of authentication. During registration, the user selects three images from the displayed set of images in the form of a 3*3 grid view. These selected images are recorded and memorized in the particular order of selection and the user is supposed to remember the images he/she selected during the registration process. During login process, the user has to select the same images selected by him during registration. If the user selects the correct images the user will be provided access for the pair based session password. If the user fails to select the correct images chosen by him during the registration process the user will not be authenticated and will have to login again with correct image selection process to proceed for pair based pair password entry. The system was tested for various users and has been verified for the authentication schemes. It has been observed that though the proposed system provides a better security, the time required for the login process is a tad bit more than a normal login procedure. But for a safer security mechanism, this indeed is a small compromise.

III. PROPOSED SYSTEM

The proposed system is a combination of two authentication schemes, namely graphical password and a CAPTCHA. The system allows the user to select an image password and create a secure password of their own. The user can choose any point on the image as the authentication portal. The user must have to remember the image that he chooses as the password during the login stage. A random number session key (CAPTCHA) is generated by the system and user has to store it for further reference during the login. The CAPTCHA consists of numerous random characters which are required during the login stage. The proposed system architecture is depicted in the above figure.

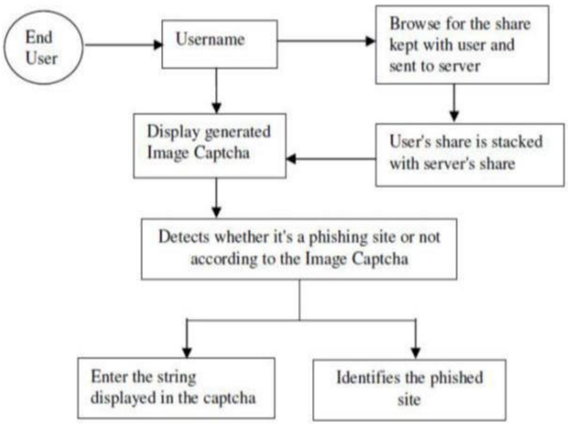
End User
Username
Browse for the share kept with user and sent to server
Display generated Image Captcha
User's share is stacked with server's share
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the captcha
Identifies the phished site

Fig.1 The Proposed System

The proposed system consists of three modules:

- User Registration module
- Image Selection and CAPTCHA module
- Login module

The proposed authentication system works as follows:

A. Registeration Phase

User registration phase includes registering the new users in to the system. For registering to the system users have to click on the "new user registration" button. It will display a registration form. For registration the users have to first enter their username and the other relevant data that is asked for in the registration form. The username must be unique to the system. The system will check whether the username already exists in the database or not. The first-time user will also have to set a password which is alphanumeric in nature and should be strong enough. The details of the user obtained from the registration form are stored in the database. After filling the registration form successfully, the user enters the "image selection" module.

B. Image Selection Phase

In the image selection phase, the user creates a graphical password by first selecting the click a point on the image (CUED CLICK POINTS). The user then chooses one more point on the image. When the user clicks on the "Next" button, a CAPTCHA will be generated which the user has to enter to validate his authenticity. This whole process is to be remembered for future reference. Finally, the user clicks on the "Finish" button to complete the registration phase.

C. Login Phase

For authentication (Login) the user first enters his unique user id (username) and his alphanumeric password. Then they click on the "Next" button. In this stage there are multiple images shown to the user and they will have to select the same image that they had clicked on during registration. Now the user will have to select the click point on one the image he had selected for security. Similarly, when they click on "Next" button the CAPTCHA key has to be entered in the box as the final step of authentication. If the clicks in each level and the CAPTCHA key are correct, only then user can successfully logon to the system. Otherwise if there is any inappropriate entry in any of the click point, the system will display an error message to the user.

D. Advantages of Proposed System

- For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Both users and websites can be identified as secure before proceeding further. Our methodology is based on the Image Captcha validation scheme using visual cryptography. It stops password and other confidential information from being leaked to the phishing websites.
- The proposed system is a combination of (n,n) image selection authentication scheme and (2,2) shared captcha authentication. Thus, it ensures multi-level authentication.

IV. CONCLUSION

Thus we propose to develop a two-way encryption based on (n,n) image selection authentication scheme and (2,2) shared CAPTCHA authentication for phishing detection and prevention, to detect the phishing websites as well as illegitimate users. It prevents password and other confidential information from the phishing websites. Important issues such as Security, and authentication will be addressed and resolved.

ACKNOWLEDGMENT

We would like to express our gratitude and appreciation to all those who proffered us the required help. A special thanks to our final year project guide, Prof. Reena Somani, whose help, stimulating suggestions and encouragement, helped us to coordinate our project.

We would also like to acknowledge with much appreciation the crucial role of the staff of Information Technology, who gave the permission to use all required resources and the necessary material for making the documents and diagrams.

We would like to appreciate the guidance given by other supervisors as well as the panels especially in our project presentation that has improved our presentation skills by their comments and tips.

REFERENCES

[1] Nagesh soradge, K. S. Thakare, A Novel anti-phishing framework on cloud based on Visual cryptography, Proceedings of 12th IRF International Conference, 29th June-2014, Pune, India, ISBN: 978-93-84209-31-5

[2] K. A. Aravind, Mr. R. Muthu Venkata Krishnan, Anti-Phishing Framework for Banking Based on Visual Cryptography, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014, ISSN: 2321-8363

[3] Amit Navarkar, D. A. Phalke, Anti Phishing using Visual Cryptography, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Volume 3 Issue 2, February 2014.

[4] Abhishek Thorat, Mahesh More, Ganesh Thombare, Vikram Takalkar, Manisha N. Galphade, An Anti-Phishing Framework using Visual Cryptography, International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

[5] Madhuri Achmani, Radhika Dehaley, Anuja Gaonkar, Anindita Khade, Two Level Authentication System Based on Pair Based Authentication and Image Selection International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 4 Issue IV, April 2016 ISSN: 2321-9653
G. Pavan N. Sameera, ANTI Phishing Framework with Visual

[6] Cryptographic and Dynamic Captcha Schemes) IJCST Vol. 4, Issue 1, Jan - March 2013 ISSN: 0976-8491 (Online) | ISSN: 2229-4333 (Print)

[7] Bhushan Yenurkar et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, AN ANTI-PHISHING FRAMEWORK WITH NEW VALIDATION SCHEME USING VISUAL CRYPTOGRAPHY

[8] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.

[9] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.

[10] Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.

[11] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[12] Real User Corporation: Passfaces. www.passfaces.com

[13] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin.