K. Madhavi *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 213-218 **ISSN: 2321-8363**
Impact Factor: 5.515

A Design Approach to Secure Data Transmission in Network Centric Warfare Systems

(A Research paper on, preventing the phishing attacks by using visual cryptography scheme and to build a strong communication channel among the various system's present in the network centric warfare system's)

[1]K. Madhavi, [2]Dr. Aruna Varanasi
[1]M.Tech 2nd Year, Department of Computer Science, Sreenidhi Institute of Science and Technology
Email - kopnamonimadhavi@gmail.com
[2]Head of the Department, Computer Science, Sreenidhi Institute of Science and Technology
Email - arunavaranasi@sreeenidhi.edu.in

Abstract: In the present modern world defense systems a huge Network Centric Warfare System (NCWS) are deployed to achieve operational efficiency. A NCWS consists of Radio Communication Systems, Radar Systems, Missile System and EW Systems. These different systems are deployed in different locations, regions and are linked together over a network. The user of the sub-ordinate systems can update software by downloading from server. As the updation of these software is based web based server there is possibility of server being attacked by hacker. To secure the central server and also to build security among different systems deployed in NCWS an exclusive anti-phishing techniques being proposed to be developed based on Image cryptography. Based on this approach, the image cryptography called Visual cryptography is used to divide the image into 'n' shares and these shares are stored at the User sub-ordinate System and at the Server during the registration time. During the each login phase for updating the software, legitimacy of a website is verified by stacking the shares of the image from the client system and server system. Using this Image cryptography methodology, both server side data and sub-ordinate systems (like radio communication system, radars etc.) will be protected. This approach protects systems from phishing attacks from enemies.

Keywords: Phishing Attack, Visual Cryptography, Mutual Authentication, Network Centric Warfare System's (NCWS's)

1. INTRODUCTION

The Network Centric Warfare System's (NCWS's), provides a integration & interconnection of all different participants (sub-ordinate system) in the warfare environment and as a very important level of information superiority enabling scheme , in the operation like creating situational awareness, helping in fast and correct decision making, generating the increased combat power by Missile system, Radio Communication system's, sensors system's, which are connected to the NCWS's in order to achieve high level tempo of the missions, and increasing in the speed of commands in between the Connected system's and degree of self-synchronization. The NCWS's , provides an efficient interactions among the system's that are connected to the central server which are deployed in different location , and are connected over a network for sharing the information among these System.

A. PHISHING ATTACKS

A computing scam, where the intruders(unauthorised person) uses several techniques in order to steal the confidential and sensitive personal information from the actual user by creating & sending fake web sites.

Phishing often starts with a legitimate looking web sites asking the user to re-enter the user's login credentials, and phone number, or other information that can used against you.

B.TYPES OF PHISHING ATTACKS

They are several different types of phishing attacks have been identified. Some of the most important phishing attacks are listed below.

i. Deceptive Phishing: Phishing is in the form of creating the fake online websites and deploying the into the victim's network ,to order to steal the victim's confidential data and attacker uses social engineering, user's victims' personal identity information and account credentials [1][2].

ii. Malware Phishing: In this type of phishing attack the intruder design's a malicious software & use it to harm or to secretly get the access of the victim's [1][2].

iii. Data Theft Phishing: Once the malicious code is deployed and it is running on the victim's system , it as the capability to directly steal users confidential data which is stored in the victims systems[1][2].

iv. Key loggers: The Key loggers are the small applications which are installed themselves either into a web browser application or as a device driver , which monitor's the confidential information that being input and send the relevant data to a phishing server[1][2].

C. VISUAL CRYPTOGRAPHY

Visual cryptography scheme is a powerful Mechanisms by which one secret image can be divided into two or more shares. When these divided shares of the image are superimposed exactly, the original image can be discovered without any mathematical calculations. There are following visual cryptography schemes [3]:

l) (n, n) visual cryptography: In (n, n) visual cryptography sharing of image , the server generates n (n 2:2) number of secret shares of the image and all these shares are needed to be stacked together in order to reveal the secret image information[3].

2) (k, n) visual cryptography: In (k, n) sharing of image, the original image that has the secret information is split into n shares and decryption of the image is impossible without the 'k' shares are superimposed[3].

3) (2, 2) Visual Cryptography: In (2, 2) visual cryptography image sharing, the server generates 2 shares from the original image and secret information will be reveal after stacking both share of the image[3].

The propose design uses (2, 2) visual cryptography scheme, each pixel P in the original image is encrypted into two sub pixels called shares.

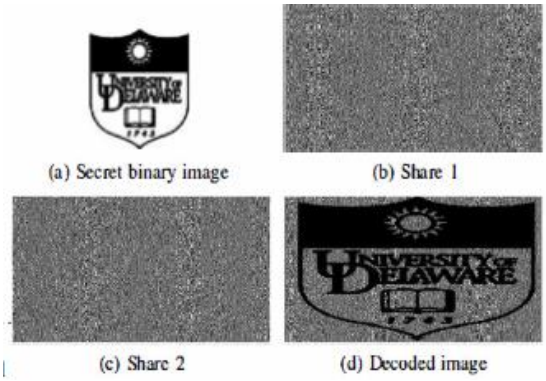

Fig 1 Basic example of visual cryptography.

The secret image (a) is encoded into two shares (b) and (c) showing random patterns. (d) is the decoded image

The rest of this paper is organized as follows:
Section 2 describes about the related work. Section 3 presents our proposed detection scheme and Section 4 describes about the determination of phishing website, conclusion and future works are given in Section 5.

2. RELATED WORK

Juan Chen et al[4], proposed a very unique standard approach. According to these approach they have design an anti-phishing algorithm based on end-host scheme, which is called Link Guard, this works by using the hyperlinks of the generic characteristics in the phishing attacks. These characteristics are derived by analyzing the phishing data archive provides through Anti-Phishing Working Group (APWG). The APWG is based phishing attacks generic characteristics, The Link Guard can not only detect the known phishing attacks but also unknown the attacks. Michael Atighetchi et a[5]l, as designed a framework which is based on attribute-based checks in order to prevent the phishing attacks. Amir Herzberg et al[6]. as tried to designed an improved security methods and in the identification of indicators, as author implemented, a browser extension in Trust Bar. Mohsen Sharifi et al[7]. gave an Anti Phishing Authentication (APA) technique to detect and prevent real time phishing attacks. Daisuke Miyamoto et al. [8] tried to study of users past trust decisions (PTDs) for improving the accuracy of detecting phishing sites[9].

3. PROPOSED DETECTION SCHEME

Visual cryptography provides a powerful technique by which one secret can be divided into two or more shares, When these shares are superimposed exactly, the original secret can discovered without any computation. The proposed approach uses visual cryptography schemes for creating "n" share of image. Client(Radar system , EW system etc.,) stores the some share of this image and some share is uploaded to the website (central server) at the time of user registration. During software updation (each login phase), a user verifies the legitimacy of a website by getting secret information with the help of stacking these shares of the image. After this, website asks for some other information like, user name and password. Using this visual cryptography techniques , legitimacy of a website and its identity can be verified by stacking the shares of the images.
Which is shown in the "Fig 2".

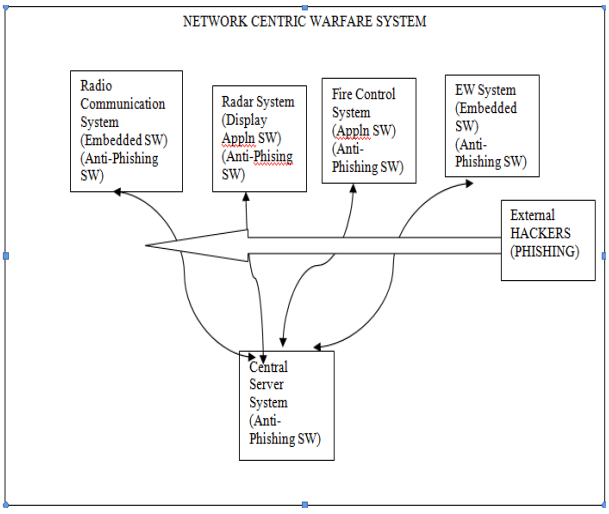

Fig. 2 proposed architecture of Network centric warfare system.

A. GENERATING SHARES DURING REGISTRATION PROCESS

The proposed approach uses (2, 2) visual cryptography schemes for creating share of original images, which is shown in "Fig. 3". In (2, N) visual cryptography, where N=2 and thus implies that the original image is split into two shares and are shared to client and to central server. These shares are required to decrypt information contained in the original image during the login process[9].

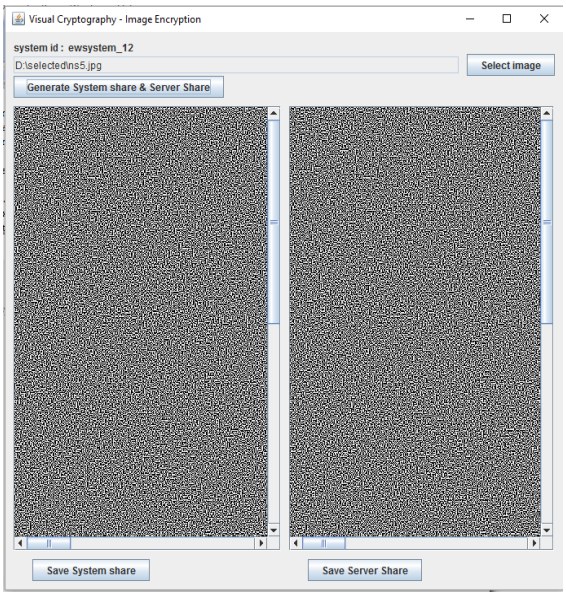

Fig.3 Generating the two shares from the original image

We will get secret information by stacking both shares while no secret information can obtained from individual share. Once a server creates the share, Share I is stored in the client side system and Share 2 is stored in the server system at the time of the user registration process. This step is very essential for all system users and cannot be ignore. The shares are linked with the unique id of the client system's . During the registration time the central server stores all the necessary details of the sub-ordinate's system likes system id, username, password and system share.

B. LOGIN VERIFICATION PHASE

During the login process in order to update the software, the user of all the sub-ordinate system are required to upload their respective share with their unique id. The server will verify the legitimacy of the user by stacking the user shares with the server share. By using these techniques we can provide mutual authentication between the all the sub-ordinate system's and central server and all prevent the system from the phishing attacks. If the system share matches with the server share then the client system is moved to the actual login page of the central server where the system can update the software by entering their credentials. And if the shares doesn't matches then the client is blocked without accessing the next pages of the application[9].

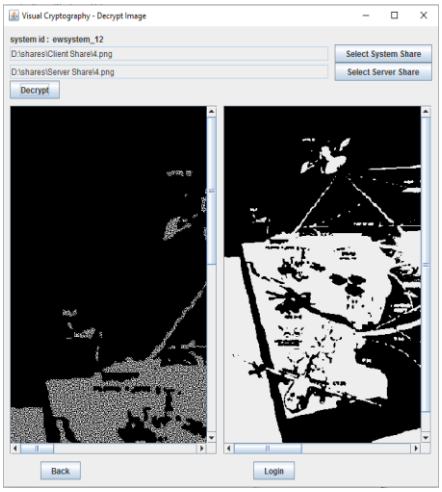

Fig.4 Stacking the client share and server share for validating

4. DETERMINATION OF PHISHING WEBSITE

Suppose if the attacker has created a phishing website, which looks like similar to the original website. As soon as user will click on suspicious links, fake website will be open, which will ask for secret key. In this step user will enter the unique secret key (client share) and wait for the desired Share2 image at a particular position because this is a fake web site, so obviously it will not have the secret information related to Share2. Since client is downloading his Share2 image from opened website and get secret information after stacking the both share. Due to absence of a secret information, user can determine that it is not authorized website and he is suffering from phishing attack. In this case, the user must open a proper website by verifying the URL and then must change his current secret key by newer one. Because attackers now aware with old secret key. Hence, we will invalidate that secret key. When a user enters correct username and password, then only he can see his account in website, So here our main aim is to protect username and password. Suppose if an attacker knows secret key, which is not changed by newer ones until now. At that condition, the Share of image does not matter for an attacker.

Now user will get login page but still unaware of username and password so he will not be able to see the account information as well as he cannot change the secret key because during changing it, an attacker must know all credentials of user[9].

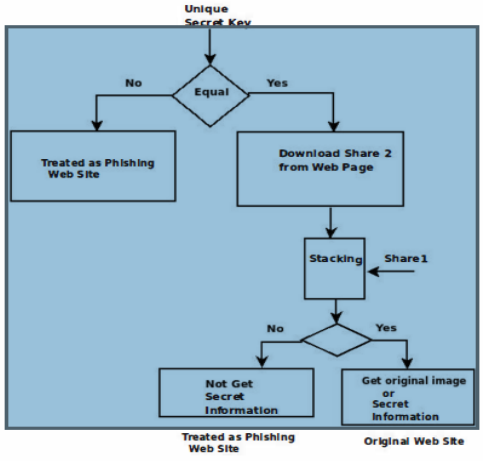

Fig 5.deteminating the phishing websites

5. CONCLUSION AND FUTURE WORK

In the present modern world, phishing attacks are so common because the intruder can attack globally and capture and store the user's confidential information likes username and passwords. This information is further used by the attackers in order to communicate with the network centric warfare system's. To secure the server and also to build security among different systems deployed in network centric warfare, an exclusive anti-phishing techniques being proposed to be developed based on visual cryptography. According to this approach the server will create two share of the image using (2, 2) visual cryptography technique. First share is stored at client side system and second share uploaded to central server at the time user registration process and also stores the details such as username, passwords, system id etc.. During each login phase, a user will verify the legitimacy of website by getting secret information with the help of stacking both shares. In the future work, proposed scheme is based on centralized approach, centralized server can be problematic when attacker will attack on the server to get the user information. So this problem can be reduced with the help of distributed sever approach.

REFERENCES

[1] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A Survey of Phishing Email Filtering Techniques," in iEEE Communications Surveys & Tutorials, vol. 15, pp.2070-2090, 2013.
[2] S. S. Tseng, K. Y. Chen, T. J. Lee, and 1. F. Weng., "Automatic content generation for anti-phishing education game," in iEEE International Conference on Electrical and Control Engineering, pp.6390-6394, 2011.
[3]. Naor, M. and A. Shamir. Visual cryptography, Advances in cryptology. Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.
[4] J Chen, and C. Guo, "Online Detection and Prevention of Phishing Attacks," in iEEE, pp.I-7, 2006
[5] M. Atighetchi, and P. Pal., "Attribute-based Prevention of Phishing Attacks," in iEEE Int. Symposium on Network Computing and Applications, pp.266-269, 2009.
[6] A. Herzberg, and A. Jbara, " Security and Identification dicators for Browsers against Spoofing and Phishing Attacks," in ACM Transactions on Internet Technology, vol. 8, pp. I -45, 2008.
[7] M. Sharif, A. Saberi, M. Vahidi, and M. Zorufi, "A Zero Knowledge Password Proof Mutual Authentication Technique against Real-Time Phishing Attacks," in Springer-Verlag Berlin Heidelberg, pp.254-258,2007.
[8] D. Miyamoto, H. Hazeyama, and Y. Kadobayashi, "An Evaluation of Machine Learning-Based Methods for Detection of Phishing Site," in Springer-Verlag ,Berlin Heidelberg ,pp.539-546, 2009.
[9]. Detection of Phishing Attack Using Visual Cryptography in Ad hoc Network ,by Vimal Kumar and Rakesh Kumar, 978-1-4799-8081-9/15/$31.00 © 2015 IEEE

