A Review on Phishing Attack in Security Detection

Raj Kumar Singh[1], Dr.Rashmi Jha[2]
[1]*Research Scholor, Magadh University, Bodh Gaya,Bihar*
[2]*Dr. Shyam Krishna Singh, HOD, Mathematics, A.N. College, Patna (M.U.)*
(Co-Author), Asst. Prof. IITM Janakpuri, New Delhi

Abstract- In the last few years a large number of internet users are increasing additionally different companies, banks and service providers are providing services online. So various sensitive and financial data are becomes online now in these days. This aspect of internet users are an evolution for us but the dark side of this advantage is too hard to accept, because of hackers and intruders are working between end clients and service providers. A secure and efficient technique is required to detect and prevent the attacks over the network transaction. In this paper we make a survey about various attacks and their problems and establish a problem statement for finding the optimum solution for the problem arises. In addition of that here we propose a system architecture for future simulation of security in internet based security.

Keywords- Internet based security, phishing, detection, system architecture

I. INTRODUCTION

In today's era everybody is using internet with the speed of Generation like 2G, 3G, 4G, and many more and above. The Internet is a system of connected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billion users worldwide. Internet is in differential part of human life. Because every age group person use it according to their interest or according to their requirement. Some of its applications like social networking sites by which anyone can connect chat or communicate over thousands of millions apart from each other. People use internet for saving their time and physical exertion by making online shopping, online banking, e-tickets and file transfer within friction of seconds by using e-mails etc. As internet shows such an advancements and facilities it also shows its dark side also. Some threats are also related to internet users. As people use internet for their convince but there are some people whose intension is to harm other users for gaining money, to take revenge or some people do so just for fun using their skill in negative directions only. Person with bad intension known as hackers, crackers, intruders or malicious users, uses their technicality into negative directions. Internet security is a branch of computer security. In this branch different types of cyber crime and miss uses of internet are tracked. As users of internet grow, frauds using internet also gain the advancement. In this study we present different types of frauds related to e-mails. As we all are using e-mails in our day to day life, for different purpose like official mails, personal mails or promotional or advertising mails. We got different mails in our inbox like advertising or promotional mails containing some offers to lure the user. This mails are not legitimate and number of peoples get trapped into such frauds because lack of knowledge about internet security. In this paper we discuss various attacks in internet based applications, their effect and detection and prevention techniques. In next section we discuss previously made efforts in the domain of providing security over internet based applications.

A. PHISHING ATTACK

A computing scam, where the perpetrators try to get sensitive personal information by sending fake web page. Phishing often starts with a legitimate looking email asking you to re-enter your login credentials, banking information, home address and phone number, credit card numbers, or other information that can used against you.

B. TYPES OF PHISHING ATTACKS

1) Deceptive Phishing: Phishing is a form of online identity theft. An attacker uses social engineering to steal victims' personal identity data and financial account credentials.
2) Malware Phishing: It is malicious software and designed to harm or secretly access a computer system without the owner's.
3) Data Theft Phishing: Once malicious code is running on the user's computer, it can directly steal confidential information stored in the computer.
4) Key loggers: Key loggers are programs that install themselves either into a web browser or as a device driver, which monitor data being input and send relevant data to a phishing server.

C. DETERMINAN ON OF PHISHING WEBSITE

Suppose attacker has created a phishing website, which looks like similar to the original one. 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 and wait for the desired Share2 image at a particular position. Determination of phishing websites are shown in "Fig. 5". If this is 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 one 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.

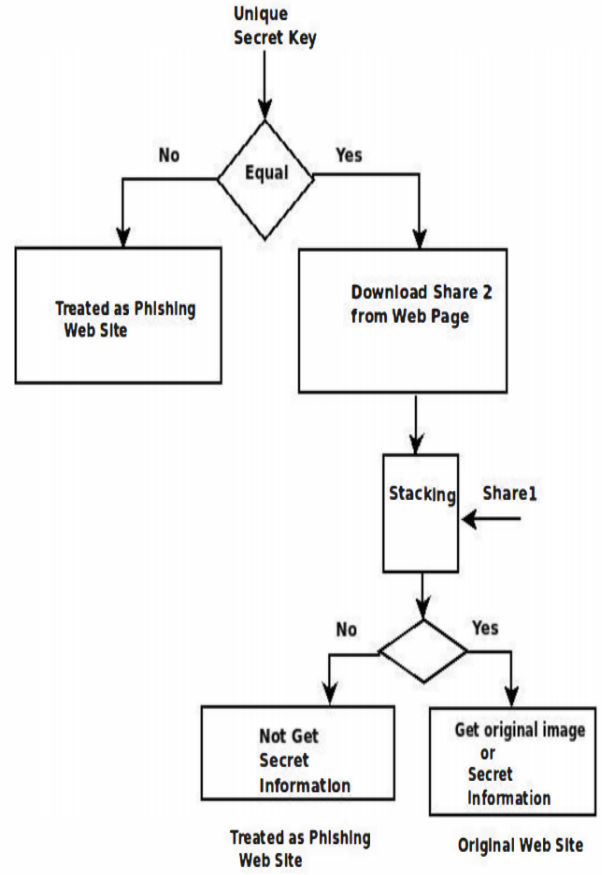

Fig.1: Determination of Phishing Web Site

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.

D. AVOIDANCE OF PHISHING ATTACK

Before being trapped into phishing attack we can work on its avoidance. After study lots of details about phishing we can avoid such conditions because of which user get into such crime. Different types are given as follows:

Suspicious Website: if user find any suspicious about

- The web site then user can check for its authenticity. By checking its https in the beginning of URL, padlock icon in the browser any sign which makes it different from original site.

•Before responding: user gets very careful to respond

Before responding: user gets very careful to respond

Before responding: user gets very careful to respond

Fantastic offer: don't believe such offers that are not

- Fantastic offer: don't believe such offers that are noteasy to believe check for the all necessary details of the web site and ask too many questions before sharing any personal detail over the internet.

•Typing of URL: never ever click on the URL given in the e-mails. Go to the URL by typing them into browser window. If there is any chance of difference in URL then it get reduced by typing it.

II. CONCLUSION

In this paper, we propose a new anti-phishing approach in ad hoc environment, which is based on visual cryptography scheme. This scheme requires online interactions with a third neither party, nor requires any plug-in or online tool hence this approach is more user friendly than previous approaches in ad hoc environment. According to this approach user will be generates two share of the image using (2, 2) visual cryptography technique. First share is stored at client side and second share uploaded to web site at the time user registration process. At the time of user registration website asked for some additional information like second share of image, user name, password and these credentials of a particular user can change once per login. During each login phase, a user will verify the legitimacy of website by getting secret information with the help of stacking both shares.

III. REFERENCES

[1]. A .P. Singh, V. Kumar, S. S. Senger, and M. Wairiya, "Detection and Prevention of Phishing Attack using Dynamic Watermarking," in International Conference on Advances in Information Technology and Mobile Communication ,vol. 147, pp 132-137,2011.

[2]. 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.

[3]. 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.

[4]. J.B.Fenga, H.C. Wub, C.S. Tsaic, Y. F. Changb, and Y.P. Chud, "Visual secret sharing for mUltiple secrets," in Elsevier, Pattern Recognition 41, pp.3572-3581, 2008.
[5]. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. "Extended capabilities for visual cryptography," in Theoretical Computer Science, pp.143-161, 201 I.
[6]. BrankaVucetic and Jinhong Yuan, Space-Time Coding, John Wiley & Sons, 2003.
[7]. Kai-Ting Shr, Hong-Du Chen, and Yuan-Hao Huang, A Low-Complexity Viterbi Decoder For Space-Time Trellis Codes, IEEE Transactions on Circuits and Systems-I, Vol. 57, No. 4, pp. 873-885, April 2010.
[8]. N.Kumaratharan, S.Jayapriya and P.Dananjayan, STTC based STBC Site Diversity Technique for MC-CDMA system, IEEE Second International Conference onComputing, Communication and networking Technologies, pp. 1-5, 2010.
[9]. Pierre Viland, Gheorghe Zaharia and Jean-Francois Helard, Improved Balanced 2n-PSK STTCs for Any Number of Transmit Antennas from a New and General Design Method, IEEE Conference on Vehicular Technology, pp. 1-5, 2009.
[10]. Kabir Ashraf, Different STTC over Rayleigh Fading Channels, IEEE Conference, Dec. 2009.
[11]. Pierre Viland, Gheorghe Zaharia and Jean-Francois Helard, Coset Partitioning for the 4- PSK Space-Time Trellis Codes, IEEE Conference on "Signals, Circuits and Systems, 2009.
[12]. Thi Minh Hien Ngo, Gheorghe Zaharia, Stephane Bougeard and Jean Francois Helard 4-PSK Balanced STTC with two transmit antennas, IEEE Conference, 2007.
[13]. Murat Uysal, and Costas N. Georghiades, On the Error Performance Analysis of Space-Time Trellis Codes, IEEE Transactions on Wireless Communications, Vol. 3, No. 4, pp. 1118-1123, July 2004.
[14]. .J.N.Pillai and S.H.Mneney, Adaptively Weighted Space-Time Trellis Codes, Southern African Telecommunication Networks and Application Conference, Sep. 2004.
[15]. HelmutBolcskei and Arogyaswami J. Paulraj, Performance of space-time codes in the presence of spatial fading Correlation, IEEE Conference, Vol. 1, pp. 687-693, 2000.
[16]. MuratUysal and Costas N. Georghiades, Error Performance Analysis of Space-Time Codes over Rayleigh Fading Channels, Journal of Communications and Networks, Vol. 2, No. 4, pp. 351-356, Dec. 2000.
[17]. M. K. Simon and M.-S. Alouini, Digital Communication over Fading Channels: A Unified Approach to Perform Analysis, John Wiley & Sons, 2000.