International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August 2013
ISSN 2229-5518

A Survey of Online Detection and Prevention of Phishing Attacks

Veena Antony[1], Divya James[2]
[1] PG Scholar,Mtech in Information System Security,IGNOU,Kochi,India
[2] Assistant Professor, Department of Information Technology,Rajagiri School of Engineering and Technology,Kochi,India
[1] veenaantony22@gmail.com, [2]divyaj@rajagiritech.ac.in

Abstract— Phishing is a kind of network attack which impacts financial loss and makes user a fool. Phishing attackers attract innocent website users by providing fake websites .In recent years phishing is a technique used for cyber crimes. In this paper we present an overview of different techniques used by the attackers and its prevention approaches.

Index Terms— Phishing, Link Guard Algorithm, Network, Security, User Protection, AntiPhishing, Spoofing

1 Introduction

In 1990,"Phishing" was emerged into the hackers' community. Phishing[1] is a theft by which attackers spread their worms and viruses into the user's machines. Also they Install spyware programs on our computer so they can monitor everything we do on the Internet and get everything about the compromised machines. Attackers used these gained information for future purpose. By Phishing spoofers collect information such as user id, password, credit card details, bank details etc.

Phishing performed through five aspects and are discussed below:

1. Try to obtain the email address of the target by several ways.
2. Attackers create the websites that are very similar to the legitimate websites.
3. Then they send the link to target email address for accessing created fake website.
4. Normal users were clicking the link and get trapped.
5. Fake website catches the user credentials and use their secret information to steal money and identity from the victims personal accounts [2].

The Tools used by the attackers for phishing are given as follows:

- Usually, we are using domain names as hyperlinks to access the website in internet. These domain names are identifiable and can easily remember. Instead of using these domain names the hackers used IP address as hyperlink and innocent users get hooked.
- The spoofers register with similar sounding DNS names, for example if the legitimate registered website is www.ebank.org,then the attacker came with www.ebanK.org .
- Set hyperlinks from the real target website if the email client software supports auto-rendering of the content.

One of the Phishing technique used by the attackers includes:

Phishing through Compromised Web servers –If a server is compromised then the attacker used that server as a tool for attacking other systems. Also if a server is compromised then a root kit or password protected backdoor can be installed by the attacker. From that onwards they can use it as a legitimate user credentials.

Currently we are using different Anti Phishing techniques to prevent phishing attacks. Anti Phishing is technique used to prevent phishing attacks. Many researchers used different techniques and approaches to prevent phishing. Here we present a literature survey for preventing online phishing.

2 Literature Survey

Many researches are working on this field and published their works based on detecting and blocking the phishing Web sites, enhance the security of the websites, block the phishing e-mails by various spam filters, Install online anti-phishing software in user's computers. In 2012, Gaurav, Madhuresh Mishra , Anurag Jain proposed an Anti-Phishing Technique Using Pattern Matrix which keeps users away from phished websites. They proposed a prevention based technique by which each website require user credentials for accessing it instead of using the hyperlinks. The users can access the website from anywhere by setting authentication using code generation and hashing [3].

Juan Chen,Chuanxiong Guo presented Link Guard based online detection and prevention of phishing attacks on WindowsXp.They designed Link Guard algorithm not only for detecting phishing but also it resist users to click on malicious and unsolicited links.The system detects the phishing up to 96% [4].

Engin Kirda and Christopher Kruegel Technical University of

Vienna, proposed an anti phishing techniques using AntiPhish algorithm. This technique tracks the sensitive information of a user and generates warnings whenever the user attempts to give away details to a web site that is considered untrusted. It is used to check the trustworthiness of a web site. The system mainly focused on web based attacks.[5]

A paper titled as "Anti-phishing Based on Automated Individual White-List" by Ye Cao, Weili Han, Yueran Le introduced a novel anti-phishing approach named Automated Individual White-List (AIWL). Automated Individual White-List (AIWL) maintains an information list about the familiar users of the websites. If an attacker tried to access the websites then it checks the list, if he is not in the list then the system alert the websites about the attacks. AIWL is effective in detecting phishing and pharming attacks with low false positive. For maintaining the white list the system uses "The Naive Bayesian" classifier .The system provides more accurate alerts to the users.[6]

International Journal of Computer Science and Technology published a paper titled "Antiphishing Model with URL & Image based Webpage Matching" by Madhuri S. Arade, P.C. Bhaskar in 2011.They suggest a new antiphishing technique based on URL domain identity and image matching mechanism. This system used two techniques i.e. URL domain identity and image webpage matching .Mainly it focused on Image Matching.[7]

According to Mallikka Rajalingam, Saleh Ali Alomari, Putra Sumari phishing can be prevented by using a Discriminative Key Point Features of WebPages. They used an effective image based anti phishing scheme to compute the similarity between images by using an invariant content descriptor, the Contrast Context Histogram (CCH). In this system they implement an image based comparison method which compares the images based on the color values. Only the creator of the that website knows about the color range of the images present in the web page and it is very helpful to identify the fake websites.[8]

In the International Journal of Information and Communication Technology Research conducted a survey regarding Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code .They propose a system for checking the web page source code. It is used to evaluate the security of the websites, and check each character in the webpage source code. It is checked by using two web page source code for legitimate and attacker website and calculate the security percentage of both web sites.[9]

3 FUTURE WORK

Phishing is serious theft in internet and anti phishing is very useful to prevent attacks. Many researchers developed different algorithms to prevent attacks from unknown clients but the prevention and detection of known attacks is unsettled. No much work is done in this area, so here we proposed a new system which detects both known and unknown phishing attacks in a platform independent manner. Also we planned to provide authentication to the system based on well known cryptographic hash algorithm MD5 [9].The architecture of the proposed system is given in the

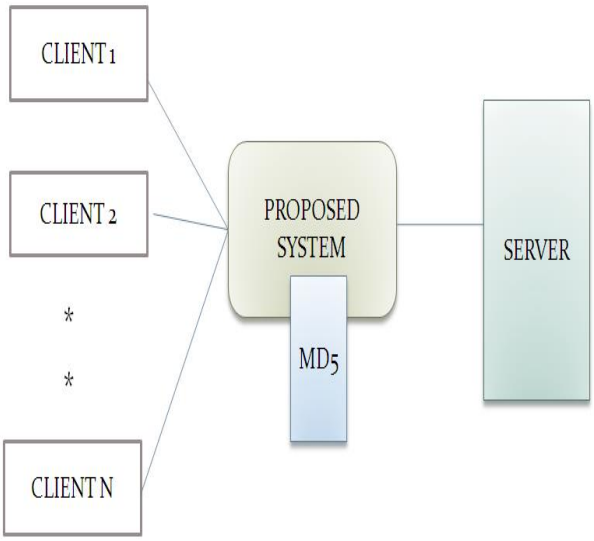

Figure:

4 CONCLUSION

In this paper we analyzed different methods used by the attacker for phishing and different techniques used by the researchers against phishing. The algorithms used by the previous researchers include AntiPhish, Code Generation, Link Guard, Image Hashing etc. From Literature survey we identified that Link Guard Algorithm is most suitable for Anti Phishing

5 REFERENCES

[1] I. Androutsopoulos, J. Koutsias, K.V. Chandrinos, and C.D. Spyropoulos. An Experimental Comparison of Naive Bayesian and Keyword- Based Anti-Spam Filtering with Encrypted Personal E-mail Message.
In *Proc. SIGIR 2000*, 2000.l

[2] http://www.w3.org/TR/xhtml1

[3] Gaurav, Madhuresh Mishra, Anurag Jain / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.1825-1828

[4] Online Detection and Prevention of Phishing
Attacks (Invited Paper) Juan Chen, Institute of Communications Engineering Nanjing 210007, P.R. China

[5] Protecting Users Against Phishing Attacks with AntiPhish ,Engin Kirda and Christopher Kruegel Technical University of Vienna

[6] Y. Zhang, J. Hong and L. Cranor. CANTINA: A Content-Based Approach to Detecting Phishing Web Sites. Proceeding of International World Wide Web Conference (WWW 2007), Banff, Alberta, Canada, May 2007: 639-648.

[7] Antiphishing Model with URL & Image based Webpage Matching Madhuri S. Arade, P.C. Bhaskar Dept. of Computer Science & Technology, Shivaji University, Kolhapur, Maharashtra, India, IJCST Vol. 2, Iss ue 2, June 2011

[8] Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages, Mallikka Rajalingam, Saleh Ali Alomari & Putra Sumari, International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (1) : 2012

[9] International Journal of Information and Communication Technology Research, Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code ,Mona Ghotaish Alkhozae, Omar Abdullah Batarfi Department of Computer Sciences, FCIT King Abdulaziz University, Jeddah, KSA, Volume 1 No. 6, October 2011