ISSN: 2321-8169
153 – 156

An Approach to the Implementation of Web Request Interceptor to Prevent Phishing Attack

Ms. Neha R. Israni
RTMNU: Computer Science & engineering
GHRIETW
Nagpur, India
nrisrani@gmail.com

Mr. Anil N. Jaiswal
RTMNU: Computer Science & engineering
GHRIETW
anil.jaiswal@raisoni.net

Abstract— Phishing attacks are growing tremendously with the growth in internet. The phishing websites appears identical to the legitimate websites and give an illusion to the user about its security. Phishing attacks that are usually carried out by sending fake e-mails or online advertising causes huge harm to the users financial as well as information security. For protecting the users against such attacks various anti-phishing strategies have been implemented having different mechanisms. This paper presents the idea of developing a custom interceptor program which will look at the Address Resolution Process and check for the authenticity and validity of resolved address and the correct URL. System will look at both local and internet based address resolution process.

Keywords*- Phishing, Anti-phishing, Internet Security, URL, IP Address.*

*****

I. INTRODUCTION

Phishing is a semantic attack which targets the user rather than the computer [1][8] is turning into a breeding ground for vast fraudulency over the internet. A term phishing was first described in detail in 1987, and the first registered use of the term "phishing" was made in 1996. Phishing is the act of sending false emails in name of legitimate organization, where users asked to enter their confidential data such as bank account details, user names and passwords. This is similar to the act of Fishing, where the fisherman catches the fish out by alluring for food on the hook and the clip inside it takes the complete fish out of the lake. Phishing attack is mostly done on online payment processors, popular social web sites, auction sites by or on the sites where users enter their sensitive information.

The act of phishing is generally carried out by either e-mail attacks or by messages which directs users to enter details at a fake website which is very similar to the legitimate one. Phishing is growing tremendously because of unawareness and because of the poor usability of current web security technologies.

Figure 1 show the phishing process, where a phisher allures the user by entering sensitive information on a fake website. From the figure it can be seen that the user is directed to the fake website while surfing the original one. A solution to this can be the checking the URL's against the DNS server, which identifies the IP addresses of the websites.

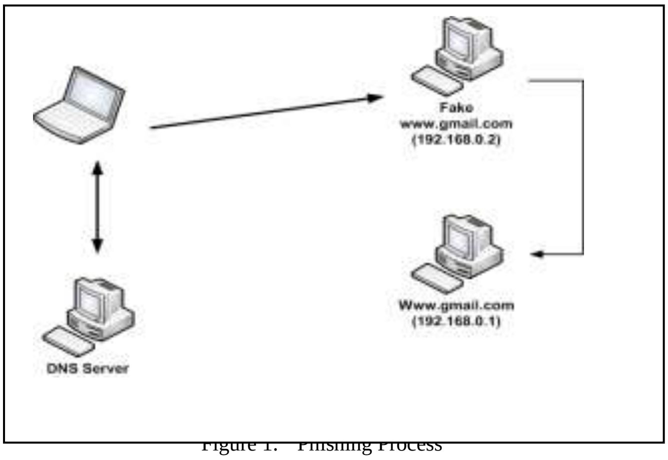


Figure 1. Phishing Process

Various attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures which can be carried out either at sever or at client side.

This paper presents a novel approach for the implementation of web request interceptor by means of a secure web browser and DNS cross checking. The rest of the paper is organized as follows: Section II reviews research work related to Phishing and Anti-Phishing. Section III presents the proposed system which is a custom web browser that checks the URL's and IP addresses against the Phish tank server. Section IV concludes the paper.

II. RELATED WORK

A. Phishing Strategies:

The main technologies of the phishing site usually go through the following procedure: l) How to distribute the information of the phishing sites to users; 2) How to trick users to make them think this is a legitimate Web site. Most phishing sites use two ways to trick the users, 'Similar Spoofing' [3] and 'Instant Spam Messages' [3].

1) Similar Spoofing [3]: This technique is used by the phishers, where the pages of the phishing sites are very similar to the legal pages. That is, the URL of the phishing sites is identical to the URL of legitimate sites, so the userswill be misguided thinking that as a legitimate Web site while visiting a phishing site.

2) Instant Spam Messages [3]: Phishers send spam messages to the users notifying them that there are some problems in their internet banking and asks them to reenter the password to solve these problems. The phishers send links which are displayed in the mail which look like the URL of the internet banking, but indeed they are anchored to a phishing site.

However, a third unrecognizable attack 'DNS-Based Phishing'[4] practiced by phishers is to tamper with industry's domain name system so that requests for URLs or name service return a fake address and ongoing communications are directed to a fake site.

B. Anti-Phishing Strategies:

A lot of work has been done in recent years on anti-phishing resulting in various anti-phishing methods. Some techniques work on emails, some aid on attributes of web sites while some on the URL of the websites.

The main anti-phishing techniques can be classified as follows:

1) List Based Methods [5]: These methods use an ever-updating list of phishing websites. Most commercial tools like browsers and security toolbars use this approach. The benefit of this method is that it requires low computational cost. Also it results in 100% accuracy on decision about websites that are present in the blacklist and produce less false positives. The main drawback is that it returns 0% accuracy when not in the blacklist. Another drawback can be large memory overhead.

2) User-Based Methods [5]: These methods involve user in the decision making by informing the users and lets the user decide the action. Thus this method requires a knowledgeable user who is aware about recent Phishing attack and one who can bifurcate in correct path.

3) Heuristic Based Methods [10]: Heuristic anti-phishing detection methods apply some heuristic rules to decide whether a site is phishing site or not. The heuristic approach may involve:

- Analyzing URL: This approach involves analyzing the URL parts like protocol, name of server, domain name, and name of server etc to decide the trueness of the site.
- Analyzing Text Contents: This approach analyses the total statistics of the page like word count, number of sentences, unique words etc. and based on the statistics the decision about the site is made
- Analyzing Visual Similarity: This approach compares the total look and feel of the redirected page with the actual web page and draws the conclusion based on similarity.
- Analyzing Image Insertion: This approach depicts the conclusion by comparison between the various images present in the redirected page and the actual page

Most of the heuristics are subjective and involves different mechanisms [10]. It can evolve from URL matching till the actual page layout.

III. PROPOSED SYSTEM

The proposed system is mainly aimed at building:

1) An anti-phishing security solution by means of developing the secure and custom web browser and phish tank server.

2) The proposed methodology is to implement network socket programming and the DNS address resolution protocol in order to get the details about URL and the IP addresses provided by user while internet surfing. This is multiple level authentication schemes for phishing detection and alert users.

The proposed system which is an anti-phishing solution helps in alerting the user while redirecting to a fake site. To incorporate such a solution a custom web browser is created which can work in normal as well as secure mode. In secure mode, the browser before directing to a website checks its phish tank server that contains the IP addresses and URL's of fake web site. Before this process, however the URL address is converted into its IP address each time for checking against the phish tank server. It is observed that sometimes the results generated can be false positive if the IP address is not presented in the Phish-tank server. Thus to enhance the security, natural language processing is used for semantic analysis of URL, where the URL's of original site and the redirected site is compared and if found dissimilar is recorded as a phishing URL. The figure depicts the overall working of the proposed system.

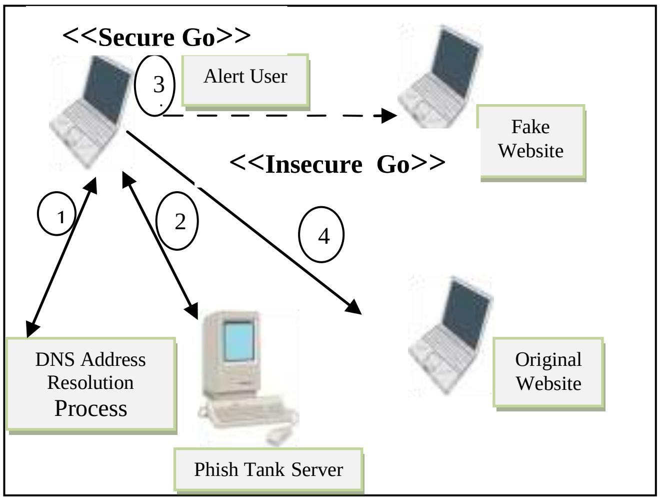


Figure 2. Workflow of Proposed System

The various components and its working is depicted below:

A) Secure Web Browser:

As system needs a control over navigating to particular web site, it requires a interception before redirection to any web site, after the name resolution process is over. We have developed a custom web browser which will allow user browse web sites and also provide security from anti phishing web sites. This web browser can work in secure and normal mode where it will take little extra time in secure mode than normal mode because it will cross check the address of every web site visiting against valid DNS server. This control will use web browser control provided by Microsoft visual studio which allow user building custom web browser.

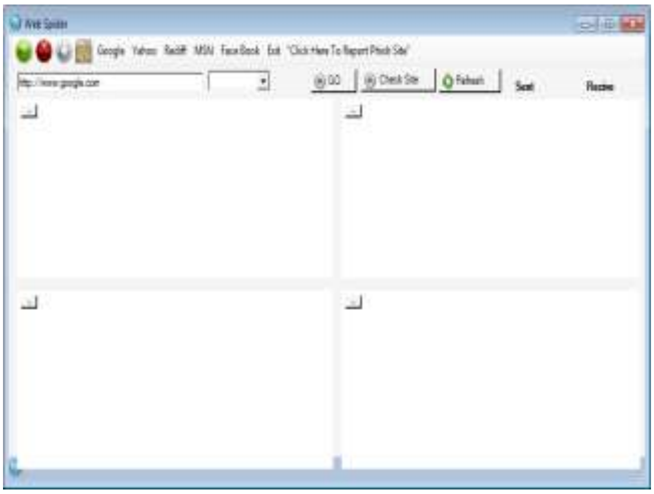
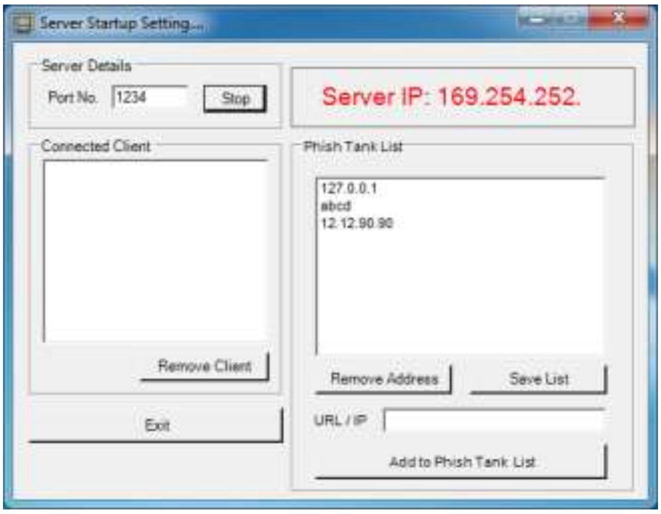


Figure 3. Custom Web Browser

B) Phish Tank Server:

In proposed system we have developed custom build server client module which will let the custom web browser communicate with the phish tank and get the details about IP address fetched and find its authenticity. It will use network or socket programming API to establish the communication between server and client. Client will create temporary connection with server on request and response basis. The custom build web browser also allow user to post IP address or URL they found as a fake in order to improve phish tank performance.


Server Startup Setting...

Server Details

Port No. 1234

Server IP: 169.254.252.

Phish Tank List

127.0.0.1
abcd
12.12.90.90

Figure 4. Phish Tank Server

C) Fake web site and Fake server:

In order to demonstrate how phishing works we have developed a phishing web site or the fake replica of well-known web site. Attack to victim machine can be shown intentionally for showing how the system re-directs user at phishing web site.

For setting up the server Internet Information Service is used. Through the "Manage site" option the fake site is installed on this server.

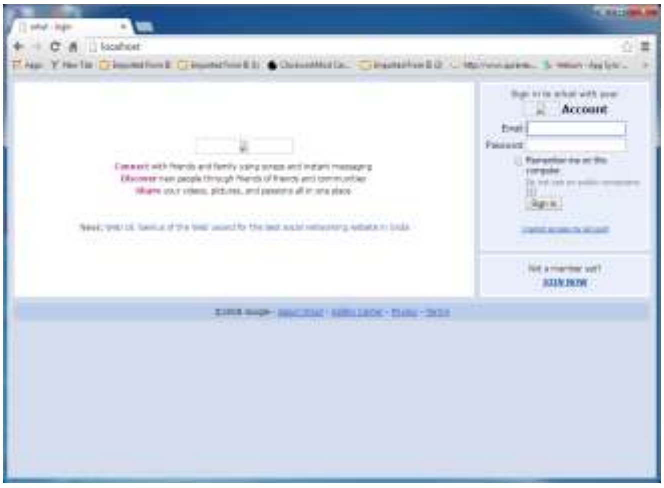


Figure 5. Mirror image of Orkut Site

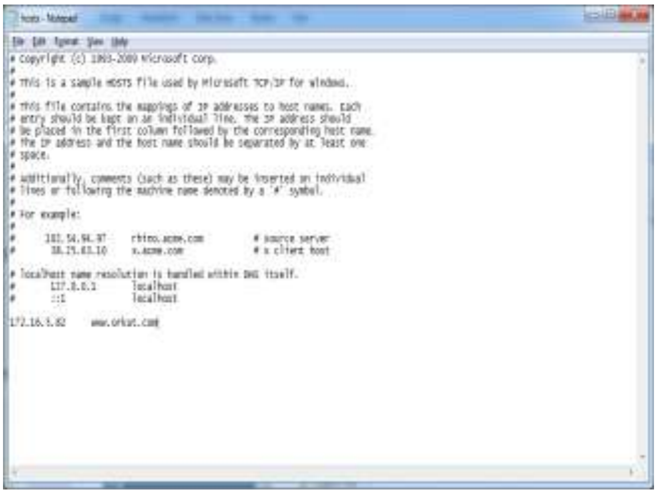
D) Use of Natural Language Processing:

Considering the interaction between computers and human, natural language Processing will be used for the Semantic analysis of the URL.

To show the effect of our anti-phishing solution two types of attacks are fashioned:

A) Affecting Local Host:

To redirect victim to fake site we need to setup victim machine's local DNS. The local DNS of the victim machine is a file located in ***"C:\Windows\system32\drivers\etc\hosts"*** and contains the local site IP's. This IP is modified with the IP address of the Fake server. Once a user visits that particular site it will be automatically redirected to the fake server where the phishing site is installed.


hosts - Notepad

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

172.16.5.82     www.orkut.com
```

Figure 6. Setting Victim's Local DNS

B) Sending E-Mail:

In this attack fake links are sent to the mail id of user tricking him to visit the URL of safe site, but however they are anchored to a phishing site.

IV. CONCLUSION

Whether it is integrated into your web browser or operates in an individual way, anti-phishing software's works in a simple but very useful way. Information about known phishing scams and phishing sites are stored in the Phish tank server. This information or the database can help in alerting you if you stumble upon a potentially dangerous site. However for physical attack on local DNS or for fake DNS entry, cross validation is done against the open DNS. In the case of a browser-based program, an alert may pop up at the top of your browser's window; in the case of individual software, an alert may pop up at the bottom of your screen. Some types of software automatically redirect you, while others give you the option of staying or leaving, our approach; however is to automatically redirect the user to the intended site.

All anti-phishing software is not created equal. Some types of software miss the mark and erroneously identify legitimate sites as phishing sites i.e. they return false positives. It pays to do a little research before downloading and installing anti-phishing software. Studies through the years have returned mixed bags of results in terms of the effectiveness of various types of anti-phishing programs. By implementing the proposed system we are trying to take better steps toward anti phishing process and the software.

REFERENCES

[1] WeiweiZhuang, Yanfang Ye, Yong Chen, and Tao Li, "Ensemble Clustering for Internet Security Applications" in IEEE Transactions on Systems, Man, and Cybernetics , November 2012.

[2] Hong Bo, Wang Wei, Wang Liming, Geng Guanggang, Xiao Yali, Li Xiaodong, Mao Wei, "A Hybrid System to Find&Fight Phishing Attacks Actively" in 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology.

[3] Gaurav, MadhureshMishra,Anurag Jain, "Anti-Phishing Techniques: A Review", in International Journal of Engineering Research and Applications" ISSN: 2248-9622 Mar-Apr 2012, pp.350-355.

[4] Ram Avtar1, Bhumica Verma2 and Ajay Jangra3, "Data Shield Algorithm (DSA) for Security against Phishing Attacks" in Research Cell: An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4.

[5] M.Madhuri1, K.Yeseswini, U. Vidya Sagar, "Intelligent Phishing Website Detection And Prevention System By Using Link Guard Algorithm" in International Journal of Communication Network Security, ISSN: 2231 – 1882, Volume-2, Issue-2, 2013.

[6] WeiweiZhuang, Qingshan Jiang, TengkeXiong, "An Intelligent Anti-phishing Strategy Model for Phishing Website Detection" in 2012 32nd International Conference on Distributed Computing Systems Workshops.

[7] Jayshree Hajgude, Lata Ragha, "Phish Mail Guard :Phishing Mail Detection Technique by using Textual and URL Analysis" in 2012 World Congress on Information and Communication Technologies.

[8] Neha Israni, Anil Jaiswal, "A Survey on various Phishing and Anti-Phishing Measures in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 01, January 2015.

[9] Yang Liu, Miao Zhang, "Financial Websites Oriented Heuristic Anti-Phishing Research" in Proceedings of IEEE CCIS2012.

[10] Rami M. Mohammad, Fadi Thabtah, Lee McCluskey, "Intelligent rule-based phishing websites classification" in IET Information Security 2014.

[11] Hossain Shahriar, Mohammad Zulkernine, "Phish Tester: Automatic Testing of Phishing Attacks" in Fourth IEEE International Conference on Secure Software Integration and Reliability Improvement.

[12] Hossain Kordestani, Mehdi Shajari "An Entice Resistant Automatic Phishing Detection", in 2013 5th Conference on Information and Knowledge Technology (IKT).