International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12-13th April 2014)

RESEARCH ARTICLE

Phish Tank-A Phishing Detection Tool

Rohan Saraf*, Mayur Khatri **, Mona Mulchandani***
*(Department of Computer Science Engineering, RTMNU ,Nagpur
** (Department of Computer Science Engineering, RTMNU, Nagpur
***(Department of Computer Science Engineering, RTMNU ,Nagpur

ABSTRACT-
Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and e-mail. Phishing is a security attack that involves obtaining sensitive or otherwise private data by presenting oneself as a trustworthy entity. Phishers often exploit users' trust on the appearance of a site by using webpage's that are visually similar to an authentic site. This paper proposes a Phishing detection technique – Anti-Phishing Enabled Web Browser, a browser enabled with anti-phishing feature to increase the level of security. Our approach includes setting up a phish tank server consisting of blacklisted websites, to avoid user accessing those sites and prevent any kind of phishing attacks by alerting the user.

Keywords: phish-tank, phishing,AOL, whaling.

I. INTRODUCTION

Phishing (pronounced "fishing") is an online fraud technique used by criminals to lure you into disclosing your personal information. Phishing is a form of identity theft in which deception is used to trick a user into revealing confidential information with economic value. Phishing attacks have deceived many users by imitating websites and stealing personal information and/or financial data.

The term "phishing" originated in AOL account theft using instant messaging, the most common type of phishing message today is email. In a typical scenario, a phisher sends fraudulent email, in bulk, claiming that there is a problem with a recipient's account at a financial institution or other business. With HTML email readers, it is also possible to provide a replica of a login page directly in email, eliminating the need to click on a link and activate the user's web browser. In browser-based attacks, it is possible to use JavaScript to take over the address bar or otherwise deceive the user into believing he or she is communicating with a legitimate site. Phishing presents direct risks through the use of stolen credentials.

There are many different tactics used to lure user, including e-mail and Web sites that mimic well-known, trusted brands. A common phishing practice uses spoofed messages that are disguised to look like they are from a well-known company or Web site, such as a bank, credit card company, charity, or e-commerce online shopping site.

Ant-Phishing techniques are the techniques which are used to combat phishing, including legislation and technology created specifically to protect against phishing. These techniques include steps that can be taken by individuals, as well as by organisations. Anti-Phishing measures have been implemented as features embedded in browsers as extensions or toolbars for browsers and as part of website login procedures. Anti-Phishing procedures include Browsers alerting users to fraudulent websites, helping to identify legitimate website, establishing secure connection, identifying the authority and augmenting password login.

An example of phishing message or mail is shown below:

"Sector 4G9E of our data base has lost all I/O functions. When your account logged onto our system, we were temporarily able to verify it as a registered user. Approximately 94 seconds ago, your verification was made void by loss of data in the Sector 4G9E. Now, due to AOL verification protocol, it is mandatory for us to re-verify you. Please click 'Respond' and re-state your password. Failure to comply will result in immediate account deletion".

II. PHISHING TECHNOLOGIES

Phishers use a wide variety of technologies, with one common thread. All technologies employed by phishers have the goal of deception.

For example:

- Deceiving a user into believing a message comes from a trusted source.
- Deceiving a user into believing that a web site is a trusted institution.
- Deceiving a spam filter to classify a phishing email is legitimate.

Phishers are technically innovative, and can afford to invest in technology. It is a common misconception that phishers are amateurs. This is not the case for the most dangerous phishing attacks. As financial institutions have increased their online presence, the economic value of compromising account information has increased dramatically. Criminals such as phishers can afford to invest in technology commensurately with the illegal benefits gained by their crimes. Given both the current sophistication and rapid evolution of phishing attacks, a comprehensive catalogue of technologies employed by phishers is not feasible.

2.1Some examples of phishing schemes include:

2.1.1 Spear Phishing: Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Prevention Technique: User should not share any personal information without verifying and checking if the site is authenticated.

2.1.2 Clone Phishing: A type of phishing attack whereby a legitimate and previously delivered e-mail content an attachment or link has had its content and recipient addresses taken and almost identical or cloned e-mail. The attachment or link within the e-mail is replaced with malicious version and then sent from an e-mail spoofed to appear to come from the original sender.

Prevention Technique: The user should not download any attachment before verifying if e-mail is an authenticated one or not and also the sender is authentic or not.

2.1.3 Whaling: Several recent phishing attacks have been targeted specifically at senior executives and other high profile targets within business and the term whaling have been coined for these kinds of attacks.

Prevention Technique: The potential targets should take preventive measures for anti-phishing and avoid sharing financial or personal information.

2.1.4 Fake e-mail messages: The message appears to be from a company that you do business with, warning you that they need to verify your account information, and if they don't get the information, your account will be suspended.

Prevention Technique: User should not respond to fake e-mail messages and also check the message if the sender is authentic or not.

2.1.5 Fake Web sites: The Web sites can be made to look similar to legitimate sites.

Prevention Technique: Authenticity of websites should be checked.

2.1.6 Fake online sales transactions: A criminal offers to buy something from you and requests that he or she pay you an amount well over the price of the item the criminal is buying.

Prevention Technique: Online transactions should be verified earlier.

2.1.7 A combination of auction fraud and phony escrow sites: This occurs when items are put up for sale at a legitimate online auction to lure you into making payments to a fake escrow site.

Prevention Techniques: User should not enter any related information at the website.

2.1.8 Urgent wording: Wording in phishing e-mail messages is usually polite and accommodating in tone. It almost always tries to get you to respond to the message or to click the link that is included in the message. To increase the number of responses, people try to create a sense of urgency so that you immediately respond without thinking. Usually, spoofed e-mail messages are not personalized, though valid messages from your bank or e-commerce company generally are personalized. The following is an example from an actual phishing scheme.

Prevention Technique: User should not click on links or lure into fake offers.

2.1.9 Fake links: People who create phishing messages are so sophisticated in their ability to create misleading links that it is impossible for the average person to tell whether a link is legitimate. It is always best to type the Web address or

Uniform Resource Locator (URL) that you know is correct into your browser. Also, you can save the correct URL to your browser Favourites. Do not copy and paste URLs from messages into your browser.

2.1.10 Homographs: A homograph is a word with the same spelling as another word but with a different meaning. In computers, a homograph attack is a Web address that looks like a familiar Web address but is actually altered. The purpose of spoofed Web links that are used in phishing schemes is to deceive you into clicking the link. For example, www.microsoft.com could appear instead as:

www.micosoft.com
www.mircosoft.com

In more sophisticated homograph attacks, the Web address looks exactly like that of a legitimate Web site. This occurs when the domain name was created by using alphabet characters from different languages, not just English.

Prevention Technique: Verify the domain name properly before accessing the website.

III. PROPOSED ARCHITECTURE

The architecture is as follows:

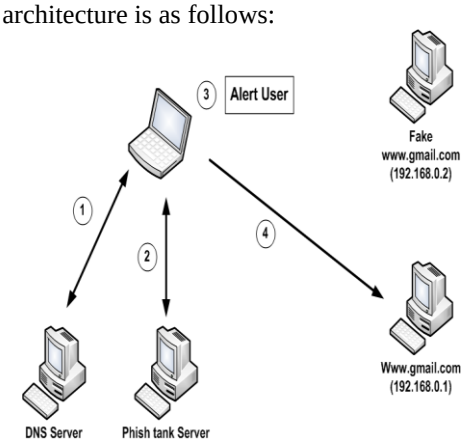


Figure 1

3.1 Working of Phish Tank Server:

The Phish tank server comprises of the list of phishing websites known as the blacklist.The particular website entered by the user is cross checked with the sites stored in the blacklist.If that particular site is the part of the blacklist then alert message is sent to the user else user is permitted to log on to that site.

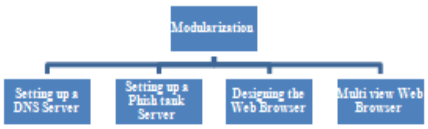
3.2 Checking the authentication of the website:

The user checks if the website is present in the phish and if the website is present in the phish tank then the user is alerted else the website is termed as authentic.

3.3 The Phish Tank list

A list is maintained in which all blacklisted websites are stored and referred later to check if a website is authentic or not, this list will be stored o the server side.

3.4 Proposed System



3.5 Responsibility of Modules

We have designed the following models for our project.

Module 1: In our first module, we set up a Domain name system server.

Module 2: Here we have built a Phish tank server, consisting of Blacklist as part of our third module.

Module 3: In this module we designed the web browser using Microsoft Visual Basic

Module 4: In this module we provide multiple views to the web browser.

3.5.1 Module 1

Step 1

Any system is capable enough; to work as a Server. As here we are making a Local Domain name system (i.e. DNS) server whose work is to manage the names of websites and other internet domains. To make any system as a DNS server, first of all we turn on all the requisite features from the windows feature section present in the control panel of the system.

Here we turn on all the internet related options like internet explorer options, internet information service, etc. This gives us the authority to get all the URL's and its IP addresses from those systems which are connected to

server's system i.e. client's system. After that we turn on telnet client and server features for the healthy relationship among client and server systems while transferring the data.

Step 2

Here we add the name of the phishing site and gave the physical path in the directory where all the credential data has to be saved.

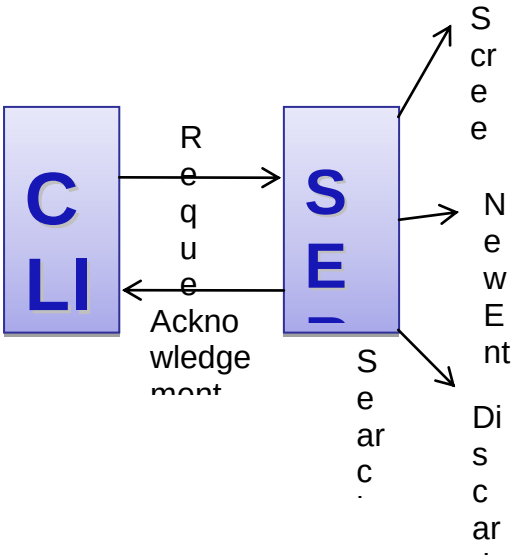
Step 3

This step is basically used to retract the user from original site IP address to the fake one. This all has been done from the hacker side.

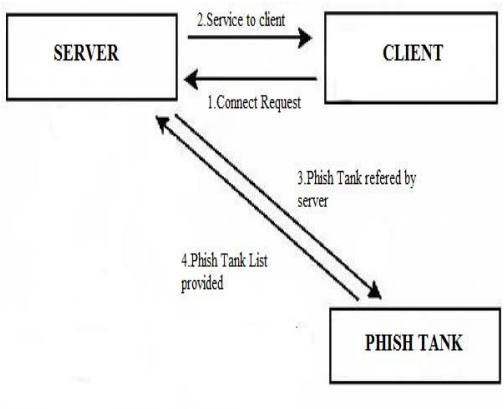
3.5.2 Module 2

In this module we are stepping towards anti-phishing technique, where we built a Phish-tank server which consists of a list of phishing sites known as "Blacklist".

Working of Phish tank server



figure

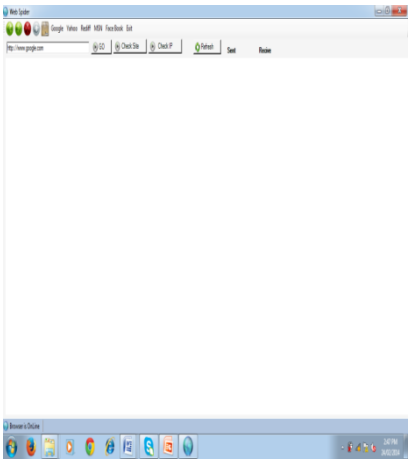


The Phish tank server comprises of the list of phishing websites known as the blacklist.The particular website entered by the user is cross checked with the sites stored in the blacklist.

If that particular site is the part of the blacklist then alert message is sent to the user and if that site. Is the legitimate one then the user is permitted to log on to that site?

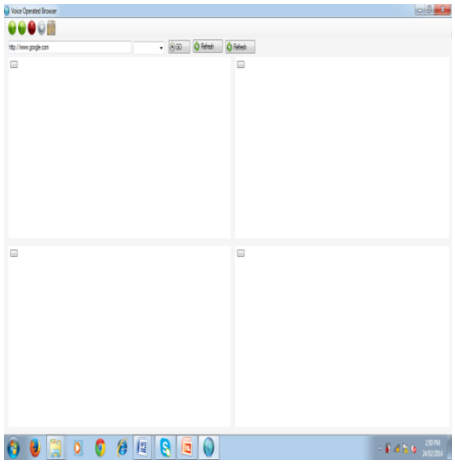
3.5.3 Module 3

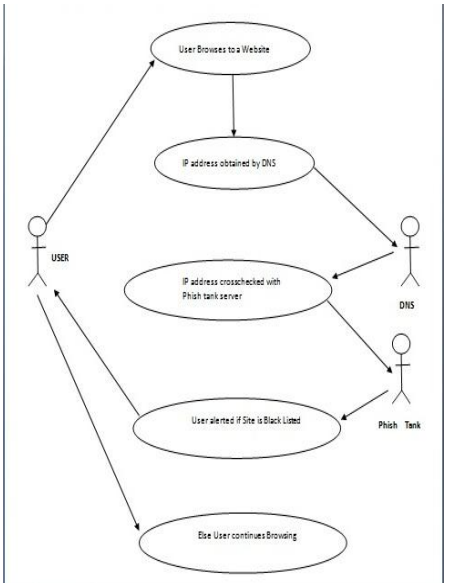
The module four comprises of designing the web browser for our anti-phishing technique to work.



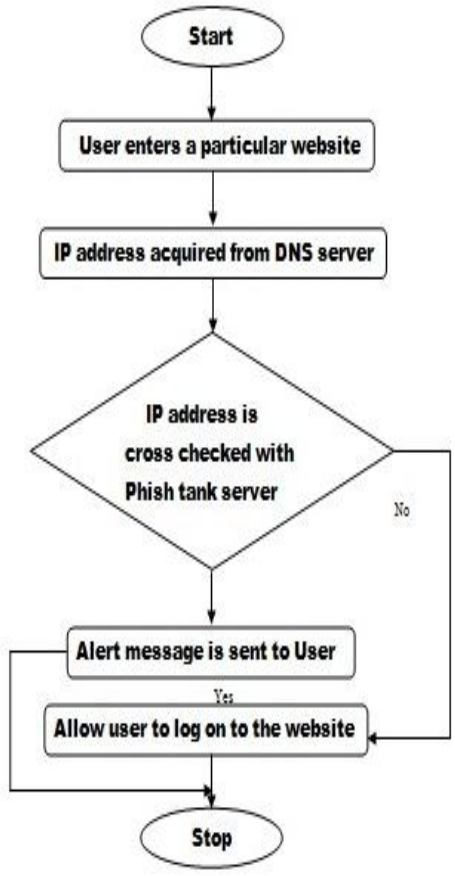
3.5.4 Module 4

This Module Involves creating Multi-views in the web browser.





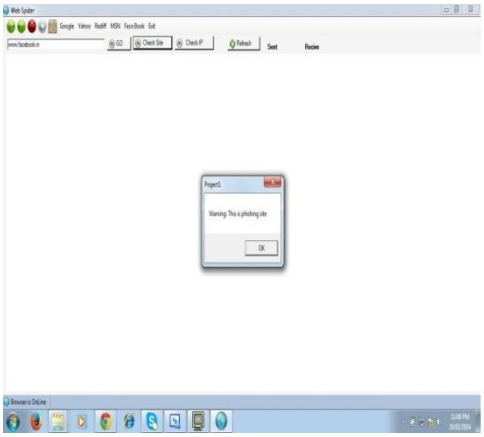
3.6 Data Flow Diagram



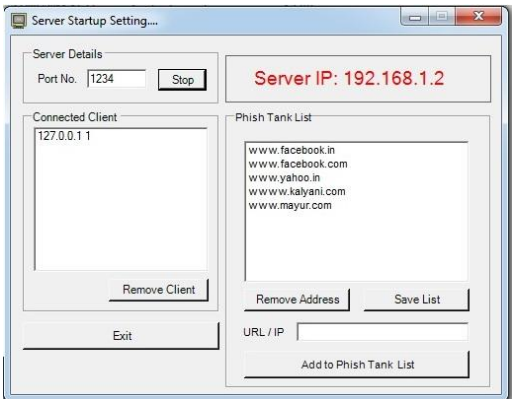
3.7 Use Case Diagram

IV. RESULTS

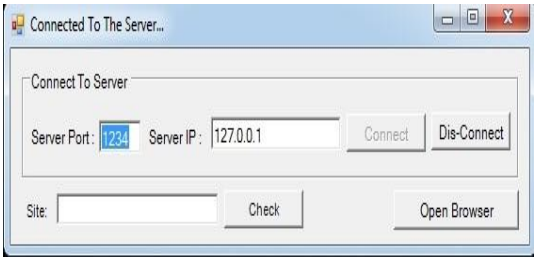
4.1 Phishing Site Warning



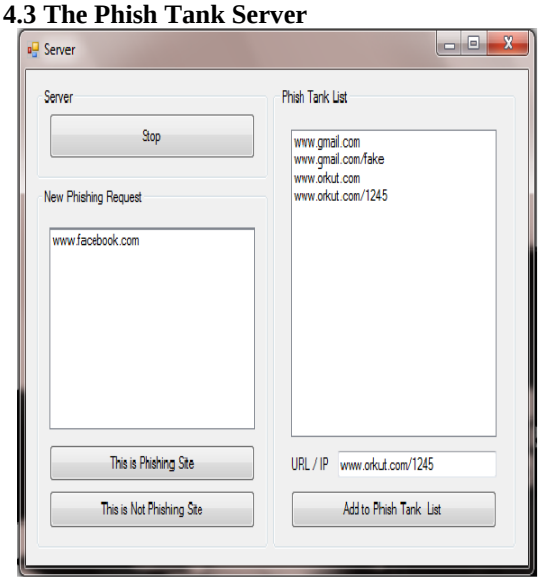
4.2 SERVER



4.3 Client Connected



4.3 The Phish Tank Server



V. CONCLUSION

The most effective solution to phishing is training users not to follow links to web sites where they have to enter sensitive information such as passwords (unrealistic!).The problem with server based solution is that crawling and black listing will find organizations in a race against the attackers.Detecting anomalous behaviours (mainly for banks) means *a-posterior* solution.An OS-level trusted path for secure data entry and transmission has the potential to dramatically reduce leakage of confidential data tounauthorized parties.AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to transmit this information to a web site that is considered untrusted.Challenge: reduce the false-positive warnings when customers use the same password in different websites.

VI. FUTURE SCOPE

Anti phishing technique implied in the web browser can also be implemented in bank websites and not only that but also on particular marked e-mails.There are number of other applications which can be added in the web browser we will be designing as part of future development such as CCTV camera screen format which enables the user to work on multiple sites at a particular instance.We can also enhance our web browser with the features of voice recognition and voice response.

REFERENCES

[1] N. Chou, R. Ledesma, Y. Teraguchi, and J.C. Mitchell, *Client-Side Defense Against Web-Based Identity Theft,* 11th Annual Network and Distributed System Security Symposium (NDSS '12), San Diego, February, 2012.

[2] F. De Paoli, A.L. DosSantos and R.A. Kemmerer. *Vulnerability of "Secure" Web Browsers.* Proceedings of the National Information Systems Security Conference. 2013.

[3] Dan Kaminsky, Black Ops of DNS. Black Hat Briefings 2007.Avivah Litan, Phishing Attack Victims Likely Targets for Identity Theft, GartnerFirstTake FT-22-8873 (May 4, 2013).

[4] Rod Rasmussen, Phishing Prevention: Making Yourself a Hard Target. Internet Identity / APWG (April 5, 2012).

[5] Blake Ross, Nick Miyake, Robert Ledesma, Dan Boneh and John C. Mitchell, A Simple Solution to the Unique Password Problem(Jul 9 2013).

[6] The Anti-Phishing Working Group (APWG) http://www.antiphishing.org

[7] Financial Services Technology Consortium http://www.fstc.org

[8] The Internet Fraud Complaint Center http://www.ifccfbi.gov/index.asp

[9] The Identity Theft Data Clearinghouse http://www.consumer.gov/idtheft