International Journal of Science and Engineering Research (IJ0SER),

Vol 6 Issue 4 April -2018
3221 5687, (P) 3221 568X

Malicious Link Identification System In Webmail Server

D.Mahalakshmi [1],S.Manisha Sree [2],D.Deena [3],P.Suresh Kumar [4]
[1,2,3] - BE Students, Department of Computer Science and Engineering.
[4] - Assistant Professor, Department of Computer Science and Engineering.
Sri Ramakrishna Engineering College, Coimbatore.

Abstract: Malicious links have been widely used to mount various cyber attacks including spamming, phishing and malware. Phishing is a type of network attack where the attacker creates a replica of an existing web page to fool users into submitting personal, financial, or password data etc. In this project, propose an anti-phishing algorithm, called Link Guard, by using the generic characteristics of the hyperlinks in phishing attacks. The link Guard algorithm is used for finding the phishing emails sent by the phisher to grasp the information of the end user. Every end user can implement with Link Guard algorithm. After the end user recognizes the phishing emails and can avoid responding to such mail. The project uses the Dot net technologies and SQL Server.

Keywords: phishing, Link guard, dot net, SQL server.

INTRODUCTION

One of the primary problems in web security nowadays is phishing. The main purpose of this attack is to gain sensitive information such as username, password, and accounts numbers.
This sensitive information can be used for future target advertisements or identity theft attacks (e.g., transfer money from victims' bank account). The primary mean of initiating a phishing attack emails. The attacker sends an email to the candidate user that contains a link beside other information. When the user clicks on the link inside the email, he will be redirected to a fake website that looks like the authenticated website, e.g. the password of credit card had been wrong for many times, or they are providing upgrading services, to allure visit their Web site to confirm or modify the account number and password through the hyperlink provided in the e-mail. If input the account number and password, the attackers then successfully collect the information at the server side and is able to perform their next step actions with that information (e.g., withdraw money out from the account).

Detection of malicious URLs and identification of threat types are critical to thwart these attacks. Phishing concept is highly used by phishers to steal user information and perform business crime activities in recent years. The number of phishing attacks increased dramatically. The analysis identifies that the phishing hyperlinks share one or more characteristics as listed below:

1) The visual link and the actual link are not the same;

2) The attackers often use dotted decimal IP address instead of DNS name;

3) Special tricks are used to encode the hyperlinks maliciously;

4) The attackers often use fake DNS names that are similar (but not identical) with the target Web site.

Proposed work is done for identifying malicious web links and identifying the type of attack by using link guard Algorithm. Since Link Guard is character-based, it can detect and prevent the phishing attacks. The implementation of the project using Link Guard algorithm in Windows XP and experiments of the Link Guard is light-weighted. Because it consumes very little memory and CPU circles, and most importantly, it is very effective in detecting phishing attacks with minimal false negatives.

RELATED WORK

These sections discuss the general procedure of a phishing attack and provide the available methods to prevent phishing attacks. Then analyze the characteristics of the hyperlinks used in phishing attacks and present the Link Guard algorithm.

EXISTING SYSTEM

In the existing system, the detection of phishing Web sites is done in time, can block the sites and prevent phishing attacks. It's relatively easy to (manually) determine whether a site is a phishing site or not, but it's difficult to find those phishing sites out in time. In DNS scanning, it increases the overhead of the DNS systems and may raise a problem for normal DNS queries, and furthermore, most of the phishing attacks simply do not require a DNS name. The phishers cannot accomplish their tasks even after they have gotten part of the victims' information.

Drawbacks

- However, all these techniques need additional hardware to realize the authentication between the users and the Web sites hence will increase the cost and bring certain inconvenience.
- Therefore, it still needs time for these techniques to be widely adopted.

PROPOSED SYSTEM

In the proposed system Link Guard Approach is used which can detect the phishing content, based on the characteristics of the phishing hyperlink. In the classification of the hyperlinks, methods collect useful information from potential victims; phishers generally tries to convince the users to click the hyperlink embedded in the phishing e-mail. A hyperlink has a structure as follows.

<a href="URI"> Anchor text <\a>
where "URI" (universal resource identifiers) provides the necessary information needed for the user to access the networked resource and "Anchor text" is the text that will be displayed in user's Web browser. The main objective of the link guard algorithm is analyzing the differences between the visual link and the actual link. It also calculates the similarities of a URI with a known trusted site. The Link Guard algorithm works as follows. In its main routine *Link Guard*, it first extracts the DNS names from the actual and the visual and then compares the actual and visual DNS names.

Advantages

- Detection of phishing content is done based on the characteristics of the phishing hyperlink.
- Link guard algorithm it works by analyzing the differences between the visual link and the actual link.

SYSTEM ARCHITECTURE

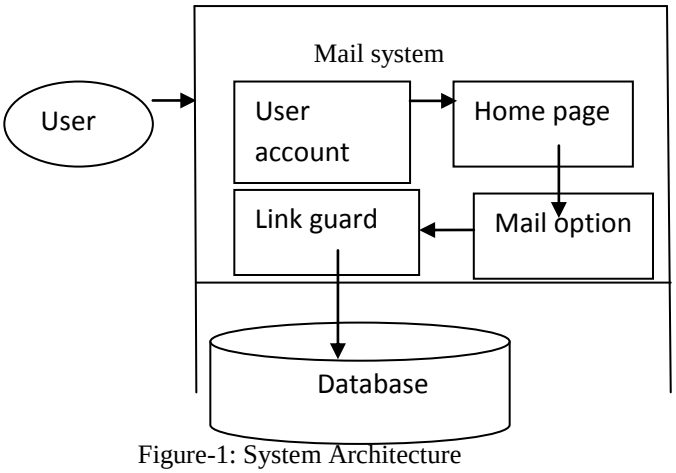

Figure-1: System Architecture

MODULE DESCRIPTION

The paper "MALICIOUS LINK IDENTIFICATION SYSTEM IN WEBMAIL SERVER" contains following modules. They are,

- Mail server creation
- User registration
- Mail composer
- Phishing checking
- Link guard algorithm

MAIL SERVER CREATION

Mail server creation is the first module in this project. Initially the mail server is created to communicate with the different persons through the email server. The mail server environment includes the option for sending email through recipient through composer option and they can receive the mail from various recipients. The mail server also has the option for viewing sent mails, spam mails and deleted mails.

USER REGISTRATION

In the user registration module initially, they have to create an account to transfer the mail to various recipients. Once the registration is completed successfully they can login

to send mails and receive mails from various users. During the registration process, the details about the individual users are gathered and stored on the server. Each and every time user login to the server and check whether the authenticated users login or unauthorized users processing.

MAIL COMPOSER

In this module, user abstraction is built. The user can send the data to the receiver using the user's mail id, subject, and content of the information or attachments of the information and can be able to send the data efficiently. The user can view the list of mails sent by the user in the sent mail folder. The mails which are reported as spam can be viewed in the spam folder. Once the mail is sent successfully the message will be indicated to the sender that the mail has been sent successfully.

PHISHING CHECKING

The received mail can be checked if it is phishing or not, the implementation of which is given in the next module. The compose mail option contains an option for spoof id. The spoof id allows the mail of the composer to be delivered with a different from address. This is being incorporated to demonstrate the Link Guard algorithm.

LINK GUARD ALGORITHM

The module contains the implementation of the Link Guard algorithm. It is possible for the user to add domain names and categorize them as either white list or black list under settings. Whenever a mail is detected as phishing the domain name in that mail automatically gets added as a blacklist. It also refers to the database of black and white list entries and sets the status of the mail as either Phishing or Non-Phishing.

SYSTEM IMPLEMENTATION

If implementation involves a production process, a manufacturing system which uses the established technical and management processes may be required.

The purpose of the implementation process is to design and create (or fabricate) a system element conforming to that element's design properties and/or requirements. The element is constructed employing appropriate technologies and industry practices. This process bridges the system definition processes and the integration process.

SCREENSHOTS

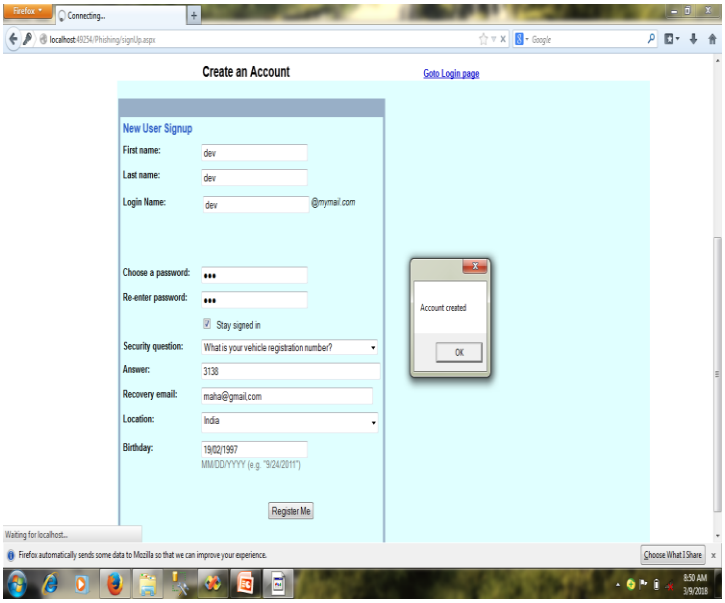

Figure-2: User Registration.

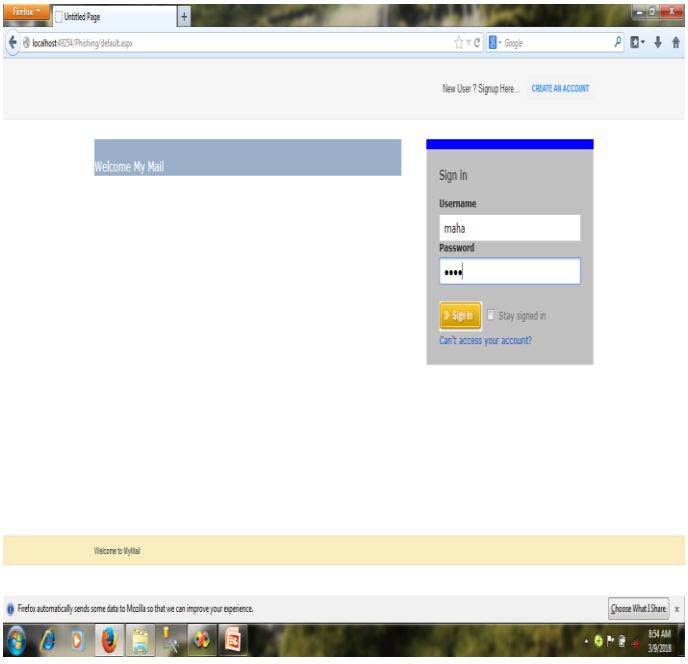

Figure-3: User login

Figure-4: View user mail details

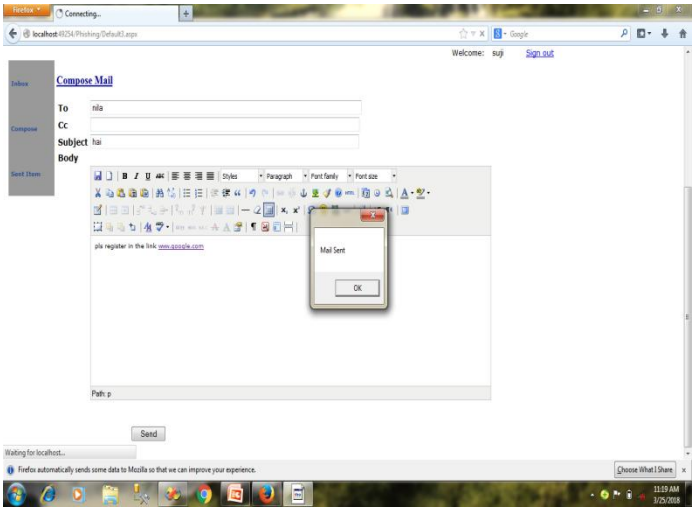

Figure-6: Sending phishing mail

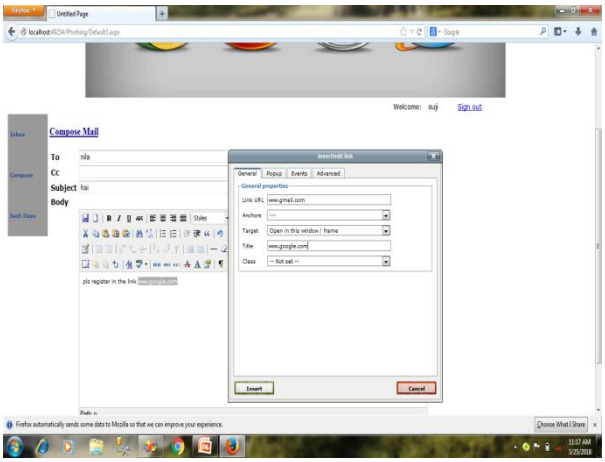

Figure-5: phishing mail

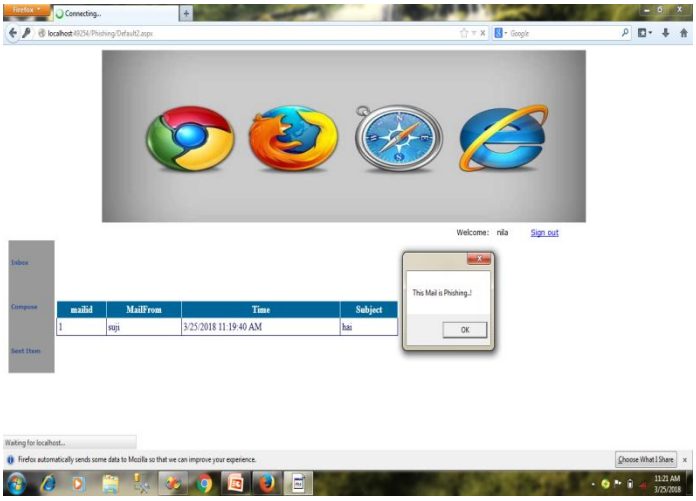

Figure-7: Identify the phishing mail

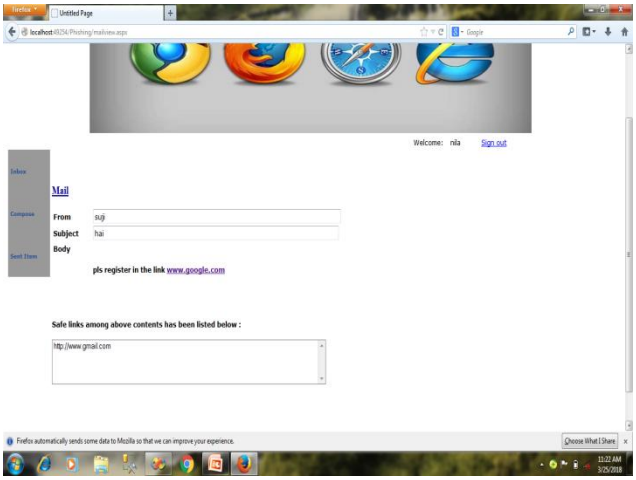

Figure-8: Identify the actual link and visual link

CONCLUSION AND FUTURE WORK

Phishing has to become the major problem in the network security. The proposed steps are highly effective in protecting E-mail users from unwanted E-mails of all kinds. Casual E-mail users could easily classify the various kinds of incoming mails and identify useless mails from the useful ones. In this paper, discuss the identification of malicious hyperlink in the mail system.

Then designed an anti-phishing algorithm, Link-Guard, based on the derived characteristics. Since Link-Guard is characteristically based, it can detect the attack effectively. We have implemented Link Guard for Windows XP. The experiment showed that Link Guard is light-weighted and can detect the unknown phishing attacks in real-time. We believe that Link Guard is not only useful for detecting phishing attacks but also can shield users from malicious or unsolicited links in Web pages and Instant messages.

As we have implemented this approach by considering the URL and Domain Identity Criteria, there are the different criteria needs to work in future.

REFERENCES

1. Abdul Ghani Ali Ahmed, Nurul Amirah Abdullah "Real Time Detection of Phishing Websites" IEEE transactions on knowledge and data engineering, 2016.
2. R. Dhanalakshmi, C. Prabhu, C. Chellapan "Detection Of Phishing Websites And Secure Transactions**"** International Journal Communication & Network Security (IJCNS), Volume-I, Issue-II, 2011 .
3. Rathore, Shashikant, Jassi, Palvi & Agarwal, Basant, (2011) "A New Probability based Analysis for Recognition of Unwanted E-mails", International Journal of Computer Applications *(IJCA),*Vol. 28, Issue 4, Published by Foundation of Computer Science, New York, USA.
4. Justin ma, Lawrence K. Saul, Stefin Savage and Geoffrey M.Voelker "Learning to Detect Malicious URLs" ACM Transactions on Intelligent Systems and Technology, Vol. 2, No. 3, Article 30, Publication date: April 2011
5. Bill Hamilton, "Programming SQL Server 2005**",** O'Reilly Media Publisher, 2006.
6. Elias M.Award, "System Analysis and Design", Galgotia Publications, Second Edition.
7. Daniel Solis, "Illustrated C# 2008", Apress Publisher, 2008.