International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

E-Mail Security System using for Phishing Attack- Using Link Gaurd Algorithm

Kalpana[1], Naveen Kuma[2], Parul Saharavat[3]
[1]M. Tech Scholer, Computer Sci. JPIET, Polytechnique, Meerut, Uttar Pradesh, India
[2]Department of Computer Sci. JPIET, Meerut , Uttar Pradesh, India
[3]D.N. Meerut, Uttar Pradesh, India

ABSTRACT

Phishing is type of cybercrime in which phisher attacker make web pages in order to trick the peoples. Phishing is a form theft in order to steal the confidential information e.g. their password, their account no. Phishing mostly uses spoofed e-mail messages that seem to come from legitimate and legal source. Trojans, malware and other malicious software are also used for phishing attacks. In this work, we proposed a new end-host based anti-phishing algorithm, which we call Link Guard plus, by utilizing the characteristics of the hyperlinks in phishing attacks. This Link Guard algorithm Plus includes one step forward with the detection of phishing measures, we introduces the part in which phishing websites is captured using the text reading to find out the malicious and threatening word to be filtered and move in the spam.

Keywords : Domain, Phishing Hyperlinks Lack List, White List, Security.

I. INTRODUCTION

E-Mail is one of the most widely and commonly used internet services. We not only use it every day for official communication but also to be in touch with our friends and relatives. Although E-Mail make our communication so easy and comfortable. Phishing was a term originally used to describe email attacks that were designed to steal our username and password. Phishing is a technique where cyber attackers attempt to fool us into taking an action provided by them.

These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entrusted you into taking an action, such as clicking on a link, opening an attachment or responding to a message. As E-Mail plays an important role in communication globally for communication and sharing of data.

The security issues also have increased. The mail infrastructure employed on the internet primarily consists of email servers using SMTP to accept messages from clients, transport those messages to **other servers, and deposit them into a user's server-**based inbox. Phishing has becoming a serious network security problem, causing finical lose and data loss. And fundamentally, phishing has made e-commerce distrusted and less attractive to normal consumers. E-Mail contains many portions for filtering on the basis of subject like Spam: sending unwanted, inappropriate, or irrelevant messages. It is often difficult to stop spam because the source of the messages is usually spoofed. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store [3].

Phishing itself is not a new concept, but it's increasingly used by phishers to steal user information and perform business crime in recent years.

II. RELATED WORK

1. **Detect and block the phishing Web sites in time:** If we can detect the phishing Web sites in time, we then can block the sites and prevent phishing attacks. It is easy to determine whether a site is a phishing site or not, but it's difficult to find those phishing sites out in time. Here we list two methods for phishing site detection [4].
2. The Web master of a legal Web site periodically scans the root DNS for suspicious Since the phisher must duplicate the content of the target site, he must use tools to (automatically) download the Web pages from the target site.
3. **Enhance the security of the web sites:** The business Websites such as the Web sites of banks can take new methods to guarantee the security of users' personal information. One method to enhance the security is to use hardware devices.

Block the phishing e-mails by various spam filters: Phishers generally use e-mails as 'bait' to allure potential victims. SMTP (Simple Mail Transfer Protocol) is the protocol to deliver e-mails in the Internet. It is a very simple protocol which lacks necessary authentication mechanisms.

Information related to sender, such as the name and email address of the sender, route of the message, etc., can be counterfeited in SMTP. Thus, the attackers can send out large amounts of spoofed e-mails which are seemed from legitimate organizations. The phishers hide their identities when sending the spoofed e-mails, therefore, if anti-spam systems can determine whether an e-mail is sent by the announced sender, the phishing attacks will be decreased dramatically [4].

Install online anti-phishing software in user's computers: Despite all the above efforts, it is still possible for the users to visit the spoofed Web sites. As a last defense, users can install anti-phishing tools in their computers [4].The Anti-phishing tools in use today can be divided into two categories:

Category I: When a user visits a Web site, the anti-phishing tool searches the address of that site in a blacklist stored in the database. If the visited site is on the list, the anti-phishing tool then warns the users. Tools in this category include Scam Blocker from the EarthLink Company, Phish Guard, and Net craft, etc. Though the developers of these tools all announced that they can update the blacklist in time, they cannot prevent the attacks from the newly emerged (unknown) phishing sites.

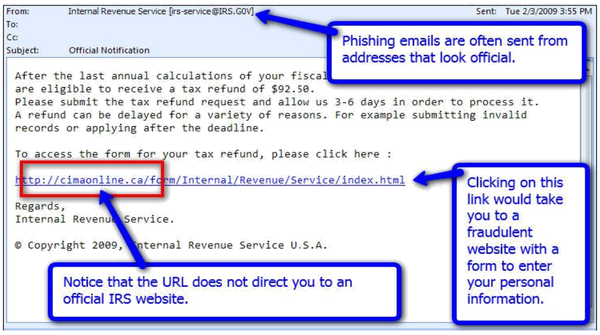
Category II: This category of tools uses certain rules in their software, and checks the security of a Web site according to these rules. Examples of this type of tools include Spoof Guard developed by Stanford, Trust Watch of the Geo Trust, etc. Spoof Guard checks the domain name, URL (includes the port number) of Web site, it also checks whether the browser is directed to the current URL via the links in the contents of e-mails. If it finds that the domain name of the visited Web site is similar to a well-known domain name, or if they are not using the standard port, Spoof Guard will warn the users.

III. PROBLEM ASSOCIATED WITH PHISHING

In our previous work the problem associated with the phishing is that how to enlist the white list and black-list. And, also how the enlist contains all the web address which we have to visit, but if mail enters our inbox how mail filter confines that this mail contains virus or any other harmful and threatening content which make harm to our data and system. In **today's** era phishing is up to the highest peak to trick the people. And most important part of phishing is to get the personal information of the bank account in order to make money transfer, or to get someone users id and password and modify the data or dteal the data (for e.g. Face book Phishing page is demand to trick the people). There are 3 types of phishing by which we can create the legitimate web page[31]:

A. Spear Phishing

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization.



From: Internal Revenue Service [irs-service@IRS.GOV]
To:
Cc:
Subject: Official Notification
Sent: Tue 2/3/2009 3:55 PM

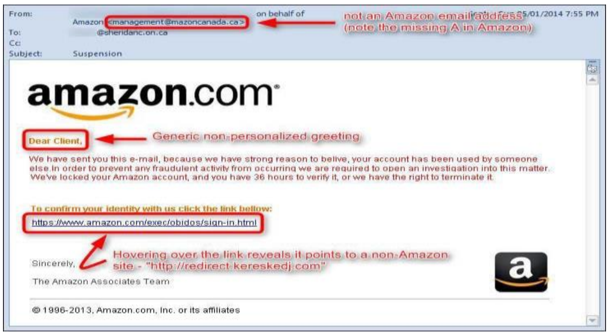
```
After the last annual calculations of your fiscal
are eligible to receive a tax refund of $92.50.
Please submit the tax refund request and allow us 3-6 days in order to process it.
A refund can be delayed for a variety of reasons. For example submitting invalid
records or applying after the deadline.

To access the form for your tax refund, please click here :

http://cimaonline.ca/form/Internal/Revenue/Service/index.html

Regards,
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.
```

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.

Figure 1. Spear Phishing



From: Amazon <management@mazoncanada.ca> on behalf of
To: @sheridanc.on.ca
Cc:
Subject: Suspension
5/01/2014 7:55 PM

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

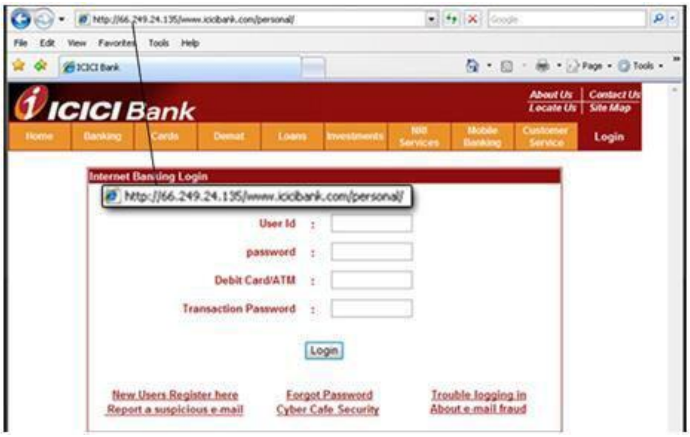
The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Figure 2. Spear Phishing

B. Clone Phishing

In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email which was delivered previously, and then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy



http://66.249.24.135/www.icicibank.com/personal/

Internet Banking Login

http://66.249.24.135/www.icicibank.com/personal/

User Id :
password :
Debit Card/ATM :
Transaction Password :

Login

New Users Register here
Report a suspicious e-mail
Forgot Password
Cyber Cafe Security
Trouble logging in
About e-mail fraud

Figure 3. Clone Phishing

C. Phone Phishing

This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source

IV. MECHANISM OF PHISHING

The following figure explains the steps involved in cracking down the personal data of users.

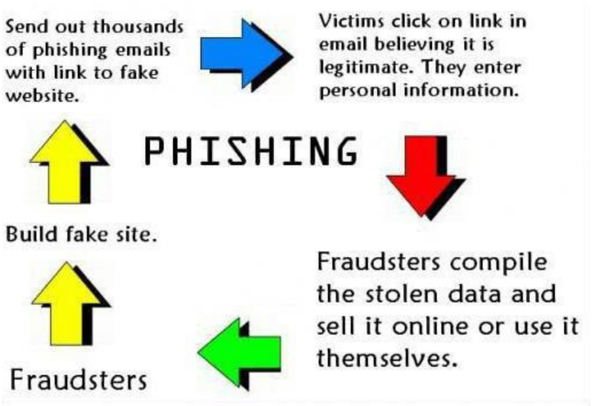

Send out thousands of phishing emails with link to fake website.
Victims click on link in email believing it is legitimate. They enter personal information.
PHISHING
Build fake site.
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraudsters

Figure 4. Mechanics of phishing

The steps followed are:

Step 1: first of all, phisher set up a counterfeited website which looks exactly like the legitimate website.

Step 2: Then a large amount of spoofed emails are sent to the targeted users in the name of legitimate banks or organization trying to convince the users to visit their website.

Step 3: User then opens the email and unaware of phishing, clicks the spoofed hyperlink in the email and enters the required information like credit card information.

Step 4: Then phisher steals the personal information from the users and perform their fraud like transferring money from the victims account.

Approaches to prevent Phishing attacks:

There are several (technical or non-technical) ways to prevent phishing attacks:

1) Educate users to understand how phishing attacks work and be alert when phishing-alike e-mails are received;

2) Use legal methods to punish phishing attackers;

3) Use technical methods to stop phishing attackers. In this paper, we only focus on the third one. It is most common and efficient method that is: using phishing

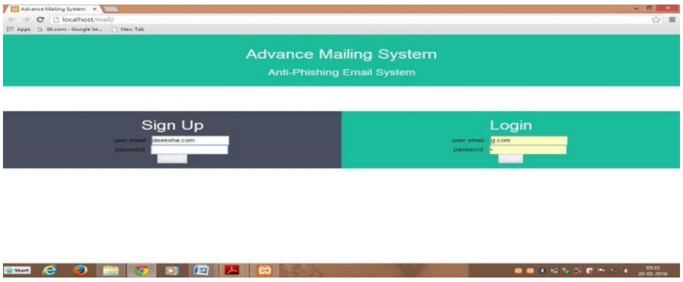
V. ALGORITHM OF PROPOSED SYSTEM

This Link Guard work is to examine the differences between the actual link and visual link. The following terms are used in the algorithm.

In this efficient link guard algorithm firstly, we have to find out the DNS names from visual link and actual link.Secondly,it compares both visual and actual DNS names, if these names are not similar then it is phishing attack for line 3 and5(Group1).We are having ip address which is said to be dotted decimal ip address, it directly used in actual_dns, then it ispossible of phishing attack in lines 6 and 7(Group2).In this algorithm it checks character wise so that it can be easily find phishing attack.

VI. CONCLUSION

An end-host based anti-phishing algorithm which we call LinkGaurd, based on the characteristics of the phishing hyperlink. Since LinkGaurd is character-based, it can detect and prevent not only known phishing attacks but also unknown ones. We have implemented LinkGaurd in Windows XP, and our experiments indicate that LinkGaurd is light-weighted in that it consumes very little memory and CPU circles, and most importantly, it is very effective in detecting phishing attacks with minimal false negatives. Link Guard detects 195 attacks out of the 203 phishing archives provided by APWG without knowing any signatures of the attack.



Advance Mailing System

Anti-Phishing Email System

Sign Up

user email: deeksha.com

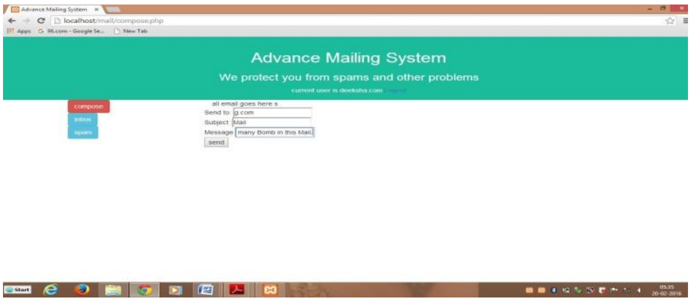
password:

Login

user email: g.com

password: *

Figure 5. Login and sign up page



Advance Mailing System

We protect you from spams and other problems

current user is deeksha.com logout

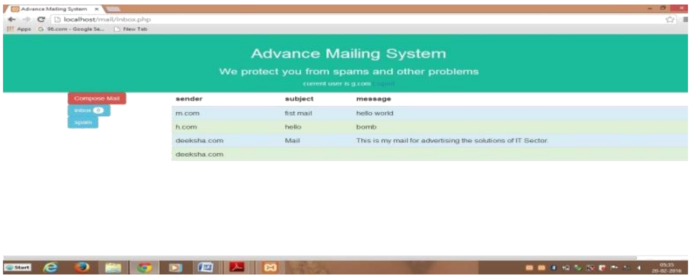
all email goes here s

Send to: g.com

Subject: Mail

Message: many Bomb in this Mail

Figure 6. Mail Page



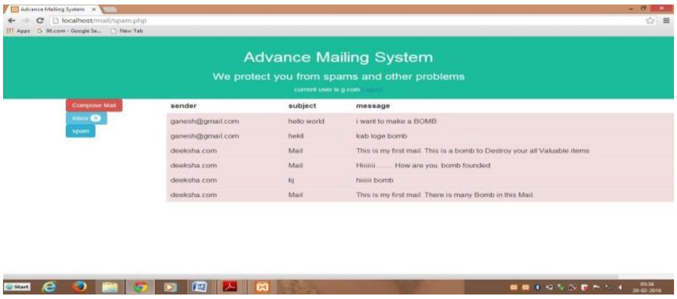
Advance Mailing System

We protect you from spams and other problems

current user is g.com logout

sender	subject	message
m.com	fist mail	hello world
h.com	hello	bomb
deeksha.com	Mail	This is my mail for advertising the solutions of IT Sector
deeksha.com		

Figure 7. Log out Page



Advance Mailing System

We protect you from spams and other problems

current user is g.com logout

sender	subject	message
ganesh@gmail.com	hello world	i want to make a BOMB
ganesh@gmail.com	hekil	kab loge bomb
deeksha.com	Mail	This is my first mail. This is a bomb to Destroy your all Valuable items
deeksha.com	Mail	Hiiiiiii........ How are you. bomb founded
deeksha.com	kj	hiiiiii bomb
deeksha.com	Mail	This is my first mail. There is many Bomb in this Mail

Figure 8. Spam Page

VII. REFERENCES

[1]. Engin Kirda and Christopher Kruegel : "Protecting Users Against Phishing Attacks with AntiPhish"

[2]. Monika Rani CSE Dept, PDMCEW: "Phishing & Anti-Phishing Techniques: Case

[3]. Study" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[4]. Gori Mohamed .J, M. Mohammed Mohideen, Mrs.Shahira Banu. N: "E-Mail Phishing - An open threat to everyone", International Journal of Scientific and Research

[5]. Publications, Volume 4, Issue 2, February 2014 1 ISSN 2250-3153 .

[6]. Preventing Phishing Attacks using One Time Password and User Machine Identification

[7]. Ahmad Alamgir Khan Senior IT Consultant, Muscat Securities Market Muscat, Oman, "Preventing Phishing Attacks using One Time Password and User Machine Identification" , International Journal of Computer Applications (0975 – 8887) Volume 68– No.3, April 2013

[8]. S.Arun, D.Anandan, T.Selvaprabhu, B.Sivakumar, P.Revathi, H.Shine Department of

[9]. Information Technology Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College/Anna University Chennai, India, "Detecting phishing attacks in purchasing process through proactive approach", Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012

[10]. Rachna Dhamija Harvard University "Why Phishing Works", To appear in Proceeding of CHI-2006: Conference on Human Factors in Computing Systems, April 2006.