ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Prevention Model For Phishing Attacks In Web Applications Using Linkguard Algorithm

A.Sarannia[1], U.R.Padma[2]

Master of Engineering, IFET College of Engineering[1, 2]

ABSTRACT: Phishing is a form of acquiring sensitive information illegally in network attack such as Banking, User names, Passwords, Credit card details and so on from users. Attackers use a combination of website spoofing and social engineering to trick a user into revealing confidential information. As the present technologies improving better, the users behind phishing scams also become more devious. Phishing attacks mostly appear as spoofed emails appearing as legitimate ones which make the users to believe and divulge into them by clicking their links provided in emails. This paper presents how to avoid the phishing scams, how it is attacked. We intend a new end-user based on anti-phishing algorithm which we call "Link Guard" algorithm. Link Guard can detect not only notorious but also unfamiliar phishing attacks. We had implemented Link Guard in windows XP. Our experiment verified that Link Guard is effective in detecting and preventing attacks.This paper uses java technologies and Oracle XE.

I. INTRODUCTION

"Phishing" is a type of Internet scams. Phishing method is characterized in detail in 1987 and it is initially emerged in 1990s.The phrase phishing was developed by Jason Shannon in the year 1995.Early hackers frequently use "ph" instead of "f" to generate new words. The illegal sites contain full of viruses, these viruses harm our computers, laptops and soon. More than 2600 websites are blocked in china because of these viruses. When phishing cunnings are increasing one common way is to login to the screen in the pop-up window, which allows to copy legal websites exactly. Phishing is the best way that criminals get all sensitive information what they need. The term is a variant of fishing probably influenced by phreaking. There are some lists of phishing techniques.

- Phishing
- Spear Phishing
- Clone Phishing
- Whaling Phishing

In these attacks we prefer spear phishing which is more under attack version of phishing attacks that combines procedure such as sufferer segmentation, email personalization impersonation of sender and other methods to avoid email filters and swindle targets into opening a link or attachment. This phishing attack may cover an entire database of all email addresses.

Link Guard is a character based uses to prevent and detect these attacks. The Link Guard algorithm is the thought for finding the phishing emails sent by phisher to grasp the data of end user. Link Guard is based on careful analysis of the characterstics of phishing hyper links. Each end user is implemented with Link Guard algorithm. After doing so end user recognizes the phishing emails and can avoid responding to such mails, since it is character based. The functions sometimes that are performed, even the URL is faked websites are similar to original websites. From the past two years the number of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

phishing attacks increased to the peak. According to the study of author Gartner, 55million US internet clients have identified them deliver of emails which is linked to phishing scams. To avoid phishing scams

- Update antivirus periodically
- Do not click on the hyperlinks in emails
- Take advantage of anti scam software
- Verify https (s-secure)
- Use anti spy ware software
- Get fundamentally educated
- Use Microsoft Baseline security analyzer
- Firewall
- Use backup system images
- Do not enter sensitive information or financial information into pop-up window
- Secure hosts file
- Protect against DNS pharming attacks

In 2004 there were 1.8million phishing attack victims. Moreover 2 million people are estimated to have been tricked into this sensitive information. In this phishing attack we can identify the phishing websites based on two lists. They are

- Black List: In this black list everything and list of things are good, we will receive everything without checking for spam because we knew everything whatever is present is good.
- White List: In this white list everything and list of things are bad, we must check it, even though if we won't check also it will be automatically deleted.

These are the two ways of filtering data which is good or bad.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. ARCHITECTURE OF DATA STEALING

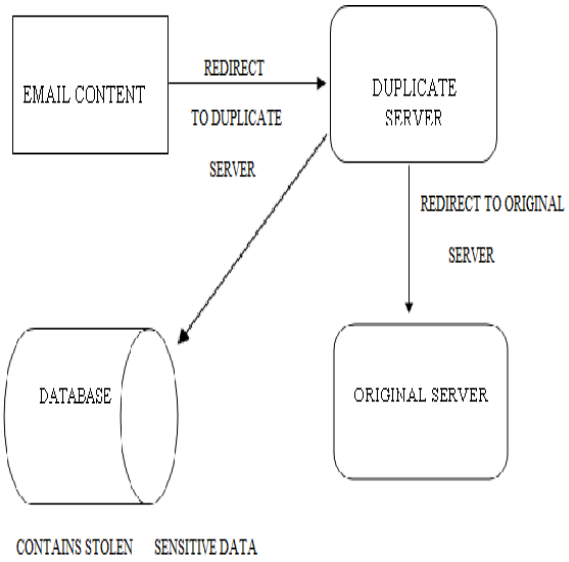

Fig. 1. Architecture of data stealing

III. LITERATURE SURVEY

- Phishing counter effectiveness and their measures, mainly using on both server side and client side in both industry and academia by swapanpurkait and vinodgupta [1]
- Enginkirda and Christopher kruegel had described protecting users against phishing attacks by using antiphish using link gua[2]
- John had described DNS based phishing attack in public hotspots [3]
- Juan chen and chuanxiongguo described online detection of phishing attacks and prevention of phishing attacks[4]
- Dhanalakshmi,prabhu and chellapan had described how to detect the phishing websites and to protect secure transaction[5]

IV. EXISTING ALGORITHM

SHA-1 is a algorithm which is previously implemented. SHA refers "secure hash algorithm". It is a cryptographic hash function which was designed by national security agency. The four different structured algorithms are SHA-0, SHA-1, SHA-2, and SHA-3. Here SHA-0 and SHA-1 contains160-bit hash values, where as SHA-2andSHA-3contain256bits.

SHA0 identifies correct error on original SHA which causes an weakness.SHA-0 algorithm is not supported by many application. Every SHA algorithm differs from every other algorithm. In this SHA we can identify the attacks but it takes many rounds to identify the theoretical attacks and also it needs the law in certain U.S Government. In SHA

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

algorithm, cryptographic algorithm is involved to protect sensitive information and to detect data corruption. This they used in Nintendo's wii gaming console for signature verification. The function involved in this SHA is the basis of SHACAL block ciphers.

At the time of implementation SHA-1 is more secure but it slow down in execution as it includes many rounds and has collisions. Because of these drawbacks we had implemented an Efficient Link Guard Algorithm.

IV. PROPOSED ALGORITHM

The previously implemented algorithm has drawbacks which could slow down the process. Link Guard Algorithm is one such algorithm which is efficient compared to SHA algorithm. This algorithm can detect not only known but also unknown phishing attacks. We had implemented link guard in windows XP. Our experiment verified that link guard is effective in detecting and preventing both known and unknown phishing attacks.

Link Guard works by analyzing the differences between actual links and visual links. It calculates the similarities of URI with a known trusted site; it contains some important systems they are:

- Communication: Input process can be collected and send all the information to analyzer.
- Database: It stores the user input URL'S, Blacklist and White list.
- Analyzer: Link Guard is the main component which is applied on link guard algorithm, all the data provided by communication and database sends all results to alter and then to logger modules.
- Alerter: Analyzer sends a warning message as soon as it receives from the analyzer and alerts the user, the analyzer receives the reactions of the user.
- Logger: All the related information is stored.

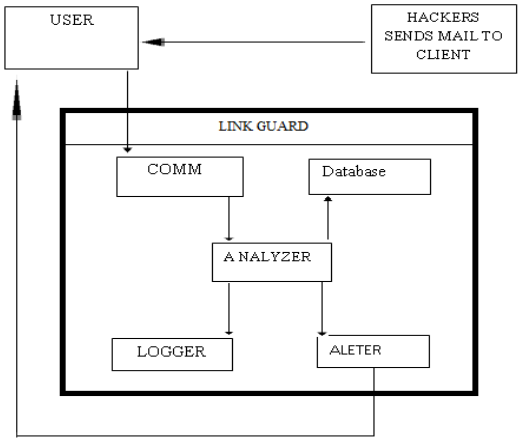

Fig. 2.Linkguard algorithm architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A. Efficient Link Guard Algorithm

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

a_link: actual link;

v_link: visual link;

a_dns: actual DNS name;

v_dns: visual DNS name;

sender_dns: sender DNS names.

intLinkGuard (a_link,v_link)

{

a_dns=GetDNSName(a_link);

v_dns=GetDNSName(v_link);

if ((a_dns and v_dns are both empty) and (a_dns ! = a_dns))

return phishing;

if (a_dns is dotted decimal)

returnpossible_phishing;

if (v_link or a_link is encoded)

{

a_link2=decode(a_link);

v_link2=decode(v_link);

returnLinkGuard (v_link2, a_link2);

}

if (v_dns is NULL)

returnAnalyzeDNS(a_link);

}

intAnalyzeDNS(actual_link)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

```
{
if (actual_dns in blacklist)
return PHISHING;
if (actual_dns in whitelist)
return NOTPHISHING;
returnPatternMatchingactual_link);
}
intPatternMatching(actual_link)
{
if(sender_dns and actual_dns are different)
return POSSIBLE_PHISHING;
for (each item prev_dns in seed_set)
{
bv=Similarity (prev_dns,actual_link);
if (bv==true)
return POSSIBLE_PHISHING;
}
return NO_PHISHING;
}
float similarity(str,actual_link)
{
if (str is part of actual_link)
return=true;
intmaxlen=the maximum string
lengths of str and actual_dns;
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

intminchange=the minimum number of changes needed to transform str to actual_dns;

if(thresh<(maxlen-minchange)/maxlen<1)

return true

return false;

}

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 and 5(Group1).We are having ip address which is said to be dotted decimal ip address, it directly used in actual_dns, then it is possible 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

When we don't have any destination information in visual link, link guard immediately calls and analyze DNS,which is used to analyze the actual dns.If the actual dns name is having black list then it is confirm that it is phishing attack. In the same manner if it in white list, then it is not a phishing attack. If it is not white list or black list then it invokes pattern matching. The unknown attacks are handled by a special feature called pattern matching. In actual link we have DNS or ip address and in visual link we don't have DNS or the destination of ip address because visual link is used future analysis.To overcome this problem we are having two methods.Firstly, phishers retrieve the data or information from email address which is similar to legal information. visual link and actual links looks similar but actual link contains legal information and visual link contains tricky information. Normally hackers use legal DNS name in the sender email address to trick the user. Secondly, we will think that all the inputted address or the data that are surfed by the user in the internet are trust worthy and we store these data in the seed set. Similarity procedure is checking the similar names with one or more names in the seed set , by invoking this procedure pattern matching checks whether the actual DNS names is different from senders address.

VI. IMPLEMENTATION ENVIRONMENT

A. Execution Setup

- Intel R core TM i3 processor-2310M CPU @2.10ghz
- main memory RAM 3GB
- operating system 64bits
- java development lit jdk 1.7.0

B.Results and discussions

When we compare with both link guard algorithm and SHA algorithm.SHA algorithm has more time complexity and it has less secure because it is having more storage capacity. Link guard algorithm has more secure and has less rounds.

Attributes	Existing algorithm	Proposed Link guard algorithm
Security	90%	94%

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Data storage	513bytes	100bytes
Number of phishing attacks	5	3
Generation time	4milliseconds	3milliseconds

VII. CONCLUSION

At present generation attacks are more in networks, phishing has become major network security problem, causing many losses by hacking the legal data that are used by the user. Phishers set their own fake websites which exactly looks like the original website including applying DNS server name, setting up web server and creating web pages similar to destination website. So in this paper we had designed link guard algorithm which is a character based. It had detected many attacks by using APWG (anti phishing working group). Link guard is implemented for windows XP, it can detect upto 96% of unknown phishing attacks. Link guard is used for detecting the phishing attacks and also malicious links in web pages.

REFERENCES

[1] The Anti phishing working group

[2] I. Androutsopoulos, J.koutsias, K.V Chandrinos, and CD.Spyropoulos. An experimental comparison of Naïve Bayesian and keyword based Anti-spam filtering with encrypted personal Email message Inproc. SIGIR 2000, 2000.

[3] Linkguard algorithm working.

[4] Ollman, G.(2004) The phishing Guie-Understanding and Preventing , White paper , Next Generation Security software Ltd.

[5] Neil Chou, Robert Ledesma, Yuka Teraguchi, D anBoneh, and John C.Mitchell. Client-side defense against web-based identity theft.Proc. NDSS 2004, 2004.

[6] Anti-phishing working group (APWG).

[7]combating web plagiarism and improving internet safety by authenticating web content by vivekpathak.

[8] web spoofing and phishing attacks and their prevention by amir Herzberg.

[9] attribute prevention of phishing attack by Michael ati

[10] A DNS monitor tool for preventing of public IP DNS rebinding attack.