Detecting the Phishing Websites Using Enhance Secure Algorithm

Shrunkhala Wankhede[1], Rajat Nikose[2], Sanket Domle[3], Shubham Asatkar[4], Jaya Singh[5]

[1,2,3,4,5]*Department of Computer Sci. & Engg.,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India*

Abstract - *Now a day, phishing attack has becoming one of the serious issues faced by internet user, organization and service provider. Phishing is the attempt to getting confidential information such as usernames, passwords, and credit card details by using spoofed emails or by using fake websites. Phishing is one of illegal activity which performs using different social engineering techniques. The internet community is still looking for the complete solution to safe internet facility from such attacks. This paper presents an overview about different phishing attacks and different techniques to keep safe. The phishing is the process used to become acquire important and confidential information such as password, credit card details or other personal information. Phishing often takes in email spoofing or sending messages. This attack will not hack any server or the website; it just creates duplicate copy of the website and tries to communicate with the user. Website based attack generate billions of dollars in fraudulent revenue of person and organization. Commonly spoofed place in the internet included EBay, PayPal, etc.*

Key Words**: *Illegal activity; Phishing attacks; social engineering techniques; spoofed email;***

1. INTRODUCTION

There are various approaches are adopted by phishers to conduct a well-planned phished attack. The victims or user of this phishing attack is mainly through the online banking consumers and the payment service providers. They are facing financial loss which eventually results in lack of trust over on the internet based payment and banking services. In order to overcome these fraud based loses there is an urgent requirement to find solutions.

Now a day's phishing attack has become one of the most serious issues faced by internet users, organizations and service providers. In phishing attack attacker tries to obtain the personal information of the users by using spoofed emails or by using fake websites or both. The internet community is still looking for the complete solution to secure the internet from such attacks. This paper presents an overview about various phishing attacks and various techniques to protect the information from the phishers.

The idea is that the bait is thrown out with the possibility hopes that a user will grab it and then bite into it just like the fish. The word phishing is the expression "website phishing" which is the variation of the word "fishing". When we compare to other cybercrimes i.e. like hacking phishing website and virus is a new kind of internet crime. Algorithms like associative and classification can be very useful in this predicting phishing websites. Thus it can provide us the queries answers about what are those important e-banking phishing websites characteristics and the indicators and how those indicators and characteristics relate to each other.

This paper develops an anti-web spoofing solution based on inspecting the URLs of fake web pages. This solution developed series of steps to check characteristics of websites Uniform Resources Locators (URLs). URLs of a phishing webpage typically have some unique characteristics that make it different from the URLs of a legitimate web page. Thus, URL is used in this paper to determine the location of the resource in computer networks. Thus it can provide us the queries answers about what are those important e-banking phishing websites characteristics and the indicators and how those indicators and characteristics relate to each other.

There are many researchers conducted to detect web spoofing attacks. However, these researches are not effective enough to stop the sophisticated attack of web spoofing. The use of various media communication such as social network leads to the increase of the numbers of attacks. 70% of successful phishing attacks are launched through social network. In fact, the lack of awareness and education on web spoofing attack causes the fall of the victims. Inability to distinguish between the fake and legitimate web pages is still a challenge in the existing prevention solutions of web spoofing.

2. Problems in existing system

In this system, we consider the requirement of improving the efficiency of filtering techniques based on Naïve Bayesian, which is a good machine learning algorithm. In this algorithm we have to input the URL which firstly compare with our train dataset. If it doesn't match then Naïve Bayesian is applies and then the keywords are extracted from the URL and after this it compare with spam as well as non-spam dictionary. On the basis of Term Frequency result the algorithm is able to predict that the given URL is spam or non-spam. One of the main drawback is it is only applicable for small amount of data. And need manual training of dataset.

3. Proposed Methodology

Web spoofing attacks occur when the user is directed to the fake web page by using fake URLs. This section describes the proposed model of phishing attack detection. The proposed model focuses on identifying the phishing attack based on checking phishing websites features. Further detail about the features of phishing websites is provided in the following subsection.

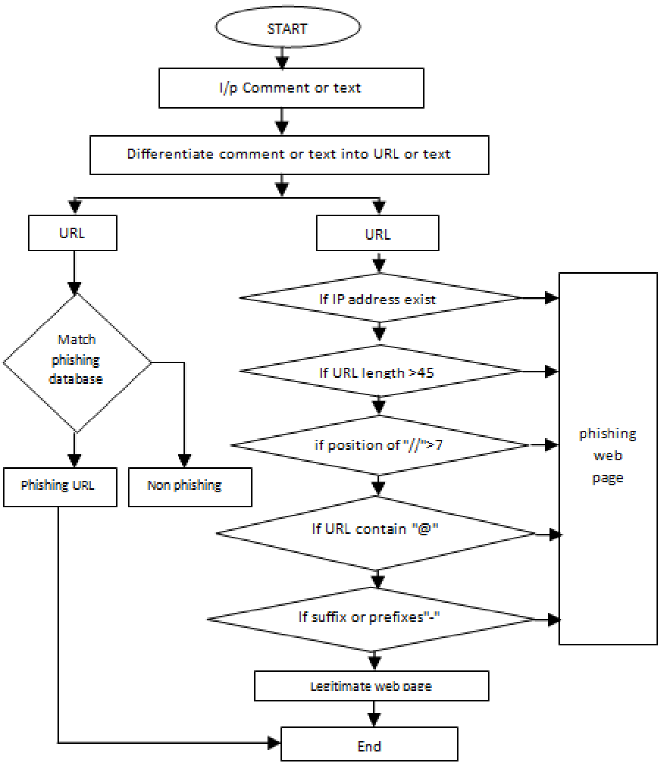

Fig -1: Flowchart of the Proposed System

3.1 Phishing Features Checking

One of the challenges faced in this research is the unavailability of complete dataset to be used as a standard for phishing websites features. According to, few selected features can be used to differentiate between legitimate and spoofed web pages. These selected features are many such as URLs, domain identity, security & encryption, source code, page style & contents, web address bar and social human factor. This study focuses only on URLs and domain name features. Features of URLs and domain names are checked using several criteria such as IP Address, long URL address, adding a prefix or suffix, redirecting using the symbol "//", and URLs having the symbol "@". These features are inspected using a set of rules in order to distinguish URLs of phishing web pages from the URLs of legimate websites.

4. Future Work

Future works of this study will include the automatic detection of the web page and the compatibility of the application with the web browser. Additional work also can be done by adding some other characteristics to distinguishing the fake web pages from the legitimate web pages. Phish Checker application also can be upgraded into the web phone application in detecting phishing on the mobile platform.

- Possible to work on large dataset.(update dataset)
- Detection of other attacks(like spoofing , DoS ,etc.)
- Efficiency and Accuracy is being improved.

5. Conclusion

Lack of awareness on phishing education makes the attack successful. Even with the help of few indicators used by the browser such as pad lock identification, lock icon, and site identity button, the user still cannot identify the attack. Web spoofing attack is not easy to detect. Even with the newest security prevention method, these attacks still occur. The main aim of this study is to help the users especially to differentiate between the legitimate and phishing web pages by using URL as an indicator. Finding of this research demonstrates its ability to identify the fake web pages based on their URLs. As a conclusion, the most important way to protect the user from phishing attack is the education awareness. Internet users must be aware of all security tips which are given by experts. Every user should also be trained not to blindly follow the links to websites where they have to enter their sensitive information. It is essential to check the URL before entering the website.

REFERENCES

[1] International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 5 Issue 09 September 2016 Page No.17823-17826 Prof. "A Survey on Various Phishing Detection and Prevention Techniques" Prof. Gayathri Naidu

[2] International Engineering Research Journal (IERJ), Volume 2 Issue 7 Page 2384-2386, 2017 ISSN 2395-1621© 2016,Server Side Security Tool to Prevent Phishing, Prof. S.N Bhosale , Akshay Kokate, Sanat Moharir, Rahul Mahamuni, Dhawal Deshmukh

[3] IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.3, March 2015, Phishing Webpage Detection for Secure Online Transactions, Sathish .S, Thirunavukarasu

[4] International Journal for Research in applied Science and Engineering Technology, "detecting phishing websites based on visual cryptography, vol. 2issue iv, April 2014

[5] International Journal of Advanced Research in Computer and Communication Engineering "An Antiphishing Framework using Visual Cryptography", Vol.4, Issue 2, February 2015