International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

Web Browser to Prevent phishing and Sybil Attacks

[1]Pavan R. Holey, [2]Deepa chaurse

[1]M.Tech CTA TIT Bhopal

[2]Assistant Professor TIT Bhopal

ABSTRACT

Phishing is the activity of fraudulently presenting oneself online as a legitimate enterprise in order to trick consumers into giving up personal financial information that will be used for identity theft or other criminal activity. Phishing is most commonly perpetrated through the mass distribution of e-mail messages directing users to a web site, but other venues are utilized as well. In this paper, proposes a web Brower – an anti-phishing tool that prevents accesses to phishing sites through URL validation (spoof guard database), lifetime of website and most visited site module. We have also given our proposed system for Detection and Prevention of Phishing. Spoof guard also examines the anomalies in web pages and uses a machine learning approach. for automatic classification. Spoof guard does not preserve any secret information and requires very less input from user. Spoof guard performs automatic classification but by taking advantage of user assistance and external repositories, hence the number of false positives is reduced by a significant value. Spoof guard is based on an approach opposite to blacklist approach removing the race between phishers and anti-phishing organizations. Spoof given in this document. Guard maintains a valid SPOOL of URLs with the mapping of corresponding IPs.We have also given a system to detect Sybil attack by mapping IP address and server name as per searching module which preserve all the details of visited sites using our browser

KEYWORDS:- Security, Web Scams, Prevention, spoof, detection, phishing attack, hyperlink detection, digital signature. Anti-phishing, spoofing.

1.INTRODUCTION

1. Phishing is a process where an attacker masquerades as a trustworthy organization in order to obtain personal financial information from an individual, and use it for malicious purposes Identity theft through phishing scams has become a growing concern. Phishing attackers use various tactics to lure or hijack a browser to visit bogus sites.
2. The easiest method to disguise the source of an e-mail and send it to the victim pretending to be a legitimate one is , E-mail Forging we introduce the Spoof guard -a novel tool that does not completely rely on automation to detect phishing. Instead, Spoof guard relies on user input to decide on the legacy of a URL. It uses external information repositories on the Internet to help the user with decision-making. Spoof guard also examines differences in web pages and uses a machine learning approach for automatic classification. Spoof guard prevents accesses to phishing sites and warns against DNS harming attacks. Spoof guard maintains a spool of valid domains with mapping to corresponding IP addresses. URL spool is encrypted by a master password. This spool is used as local DNS file for name IP resolution.
3. According to the statistics provided by the Anti-Phishing Working Group (APWG, in March 2010, email reports received by APWG from consumers were 30,577.The number of unique phishing sites detected ,in March 2010 were 29879.Payment Services returned to being the most targeted industry sector after Financial Services held top position during H2 2009. However, the category of ‚Other' rose from 13 percent to nearly 18 percent from Q4 2009 to Q1 2010, an increase of nearly 38 percent. Amongst the affected industry sector Payment services hold 37% and Financial services 35.9%. Hence It also verifies the email details that a mail server throughout uses for the validation purposes which will restrict the opening of spoofed emails
4. To prevent Sybil attack our system will first preserve all the details of visited sites in database and using searching technique our system will check the sever name ,IP address, creation date modification date, expiry date of visited sites.

This paper has emphasized over the two main concepts which are divided into two broad categories as

1. **URL validation**
2. **Searching Module**

2.LITERATURE SURVEY

Antiphish [1] stores mapping of secret information with mapping to corresponding domain, but it is not good idea to store secret information which is memorized by user. Anitphish cannot protect user against harming attack and to keep their secret information could be irritating work for user. PwdHash [2] authenticates a user with domain specific password. It computes hash of password with domain which is used as site specific password. But it is susceptible to offline dictionary attack and harming attack. It is observed that Sybil attacks are mostly performed while using internet through web browser in whish attacking machine change their identities on network Components and layers of websites phishing criteria

Criteria	Component	Criteria
URL & domain identity (weight = 0.3)	Using the IP address abnormal request URL abnormal URL of anchor abnormal DNS record	Layer 1 sub weight = 0.3
Security & encryption (weight = 0.2)	using SSL certificate certification authority abnormal cookie	Layer 2 sub weight = 0.4
Source code & java script (weight = 0.1)	redirect pages straddling attack pharming attack using on mouse over to hide the link	
Page style & contents (weight = 0.1)	spelling errors copying website using forms with submit button using pop-ups windows disabling right-click	Layer 3 sub weight = 0.3
Web address bar (weight = 0.1)	long URL address adding a prefix or suffix using the @ symbol to confuse using hexadecimal character codes	
Social human factor (weight = 0.1)	much emphasis on security and response public generic salutation buying time to access accounts \	

3. PROPOSED MODEL

3.1 URL Validation

3.1.1. Spool Look-Up Module:

The Initial look-up module looks up the domains of URL in URL spool and picks up the corresponding IP from the URL spool if domain is found in URL spool. URL is passed to URL validation module if URL is not found on URL spool.

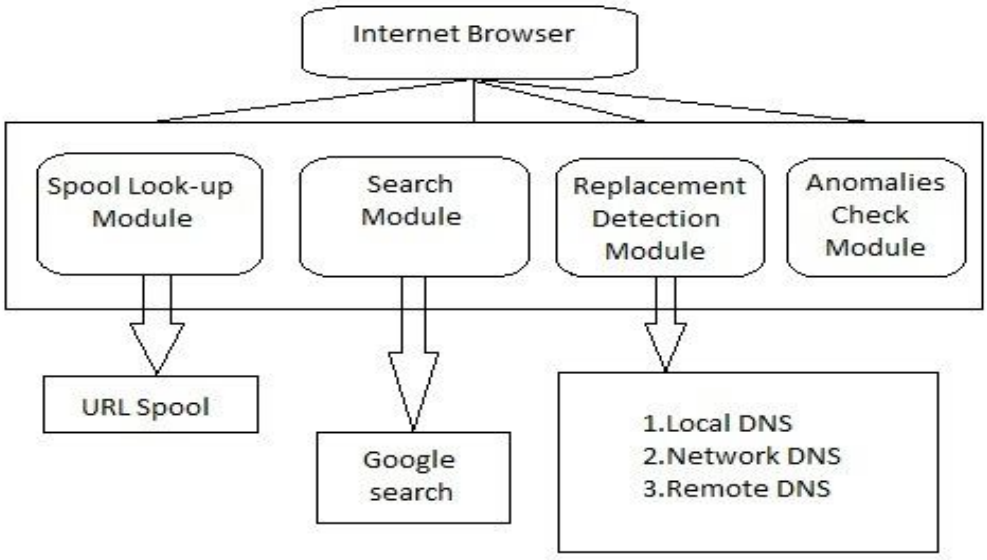

Fig. URL Validation

3.1.2. Search Module:

URL validation module issues a search query to Google for The URL. If the top 10 search results contain the URL, then it infers that the URL is legitimate. The average life time of a phishing site is 5-6 days . The fact that the site appears in the top 10 search results means that the Google crawler indexed the site, and that the site is not short-lived. Sometimes, the user reaches a web page by navigating to it from the Google search page. These domains are automatically added to URL spool after performing harming detection. If URL is not found in top 10 results, Spoof guard involves users to specify the search term for the web page they intend to visit. Spoof guard performs a Google Search and provides the search results to users. Users can choose a URL from the search results. After URL validation it URL is passed to Harming detection module with mapping to its IP and web page is retrieved from the server. After retrieving the web page Anomalies Check module examines the page. And arms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

3.1.3. Comparison Module:

In comparison module we will perform comparison of details data about visited sites maintained in database ,if this comparison breaks our rules of validating then we will warn user of our browser that phishing or Sybil attack can be made in this way we can detect phishing and Sybil attacks

ACKNOWLEGDEMENT

We express our gratitude towards those peoples who have contributed for the successful completion of this paper directly or indirectly. We are also thankful to those who shared their valuable knowledge over the same topic and given us their time.

4.CONCLUSION

Phishing have brought a dramatic increase in the number and sophistication of attacks involved in stealing user's secret information. This paper presents Spoof guard for preventing user from filling out web phishing forms. Spoof guard asks user's input to disambiguate between legitimate and phishing sites and Internet repositories of information to assist the user in decision making process. Spoof guard does not preserve any secret information as information preserving approach completely dependent on user. Spoof guard merges user assistance with automatic classification reducing the false positives by a significant value. Spoof guard uses some new features and uses a machine learning approach (Artificial Neural Network) for automatic classification and achieves 97% accuracy. Though the best measure available against such scams is user awareness, it is highly impossible also. So many tools have been developed to fight against the e-mail phishing attacks. To contribute in this regard we, have also taken a step ahead. This paper gives the details literature survey of the approaches till now used by different people to detect and prevent e-mail phishing attacks. We have given the details of how e-mail phishing attacks are carried out with experimentation results. We have also proposed our own approach to fight against the e-mail phishing attacks. The modules include the detail specification of their functionality. Thus, we assure that this solution will help to the normal end user as well as the corporate people also to send the highly confidential data. More functionally can be added to Spoof guard for protecting user against key-loggers and screen-grabbers and client side scripting attacks. Spoof guard uses Google search to

validate a URL which can be refined by using more external repositories such as Yahoo search etc. Spoof guard uses artificial neural network approach and achieves 97% accuracy. This can be improved by adding more rules and using other machine learning approaches.

REFERANCES

[1] McAfee, ―Understanding Phishing and Pharming□, McAfee White Paper, 2006.
[2] E. Kirda and C. Kruegel, ―Protecting Users against Phishing Attacks with AntiPhish□, 29th Annual International Computer Software and Applications Conference, ACM Press, Washington, USA, 2005, Vol. 01, pp. 517-524.
[3] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C.Mitchell, ―Client-side defense against web-based identity theft□, 11th Annual Network and Distributed System Security Symposium, ACM Press, Ontario, Canada, 2004, Vol. 380.
[4] L. Sean M. Allister, E. Kirda, C. Kruegel , ―On the Effectiveness of Techniques to Detect Phishing Sites □, Proceedings of the 4th international conference on Detection
[5] B. Adida, S. Hohenberger, and R. L. Rivest, ―Fighting phishing attacks: a lightweight trust architecture for detecting spoofed emails,□ February 2005, draft.
[6] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. Protecting people from phishing: the design and evaluation of an embedded training email system. In CHI ’07: Proceedings of the SIGCHI conference on Human factors in computing systems, pages 905–914, New York, NY, USA, 2007. ACM.
[7] Wilfried N. Gansterer, David P¨olz,□ E-Mail Classification for Phishing Defense□.
[8] Weider D. Yu Shruti Nargundkar Nagapriya Tiruthani,□ **PhishCatch – A Phishing Detection Tool”,** 2009 33rd Annual IEEE International Computer Software and Applications Conference.
[9] Phishing Activity Trends Report, 2009, Available online: http://www.antiphishing.org/reports/apwg_report_ 2009.pdf