Report on the fishing alarm project

Science, Computer Science

Phishing Alarm

Phishing is a type of social engineering attack where the attacker tries to imitate the original website to steal the user’s sensitive data like login credentials, credit card numbers SSN numbers, etc. The attacker lures the victim to enter his personal data by masquerading as original website. The information is then used to access important accounts and can result in identity theft and financial loss. No specific solution is implemented till date to counter the phishing attacks effectively. In this paper we exploit the visual similarity features like CSS of html document and the discrepancy between the claimed domain of the suspicious web page and the benign web page to detect a phishing attack.

Introduction

Phishing is the type of computer attack where the attacker manipulates the victim in order to persuade them to enter the user credentials via electronic communication channels, this information is further exploited by the attacker. Colin Walker has defined Phishing as- “ We define a phishing page as any web page that, without permission, alleges to act on behalf of a third party with the intention of confusing viewers into performing an action with which the viewer would only trust a true agent of the third party”.

The criminals who wants to obtain the user data creates the unauthorized replicas of the legitimate websites and e-mails, usually some financial corporate that handles the financial data of its clients. The e-mails and website will be created using the logos and the trademark of the actual website. The flexibility of HTML document makes it very easy to copy the images or even an entire document, this is fact is abused by the criminal. Phisher then sends these spoofed e-mails to as many users as possible in order to lure them into some scheme and retrieving user credentials from them. When the user finds these e-mails having logos and trademarks of actual organization, they click the links in the mail and are redirected to the spoofed website, appearing to be the actual website.

History

The phishing attack was first done by a group of hackers and pirates via America Online or AOL. These attackers called themselves ” the Warez community”. In early 1990 they created an algorithm to generate random credit card numbers, using which they attempted to create phony AOL accounts. When they hit match to the real credit card number, they were able to create an account and spam in AOL community. AOL was able to stop the random credit card generators by 1995, till the time. Then again Warez group found other ways to pretend specifically as an AOL employee and hence messaging people via AOL messenger for their information. This problem grew so quickly that on January 2 1996, the word ” phishing” was first posted in a Usenet group dedicated to AOL. AOL further included warnings on all its emails and messages to alert the users of potential phishing risk.

Phishing Attack Statistics

Phishing continues to grow rapidly taking its firm roots in the field of identity theft and thereby causing large number of frauds and scams on daily basis. There have been nearly 33, 000 phishing attacks globally per month in the year of 2012, accounting a total loss of $687 million. In June 2004, Royal Bank of Canada notified customers that fraud e-mails pretending to originate from the Royal Bank were being sent out to customer asking to verify their account numbers and Personal Identification Numbers (PINs) through a link. The fraudulent e-mails stated that if the receiver did not click the link and enter his details his account would be blocked. These e-mails were sent within a week of computer malfunction that had blocked the update of customer accounts. Financial service organization is most likely target of the attacker for phishing. The United States continued to be the top country hosting phishing websites during the third quarter period of year 2012. This is due to the fact that United States hosts a large percentage of websites and domain names overall.

Related Work

1. BlackList/Whitelist based detection

   This method of detection is most widely used in browsers such as Google Chrome and Mozilla Firefox for safe browsing. Depending on the method of implementation either the user maintains a list of whitelist and blacklist URLs or the browser automatically updates the lists. The blacklisted URLs contains the list of websites that are found malicious by the browser. Classifiers such as Naive Bayesian, SVM etc. are used to maintain the whitelist of the websites that safe for user browsing. Although easy to implement it faces the issue of high false negative ratio due to short lifetime of phishing web pages. The main drawback of this approach is that they are not effective on the web pages which were previously undetected and hence the list needs to be maintained frequently to have a good accuracy.

2. URL based detection

URL based approach analyzes the URL features of the given web pages and based on this features a decision is made whether the website is phishing or not. [3]URL features such as length, path, hostname, no. of tokens present are different for a legitimate and a phishing website. This property is exploited in this approach. Lexical analysis is performed on the URL in order to extract URL features. To maintain and update the feature list of URL properties, a classifier is employed that can successfully distinguish between the features of actual website and a malicious website and thereby can make an appropriate decision for the suspicious webpage’s URL.

3. Content based detection

In content based detection, the visual similarity between a malicious page and target page is the key feature to detect phishing attacks. The visual features considered can be text and styles, images and the overall appearance of the web pages. The study proposes an algorithm that detects the phishing pages on basis of contents of the web-page, using term frequency – inverse document frequency (TF-IDF). This cannot be resilient to evasion as the attacker can change the contents and still may make feel the website as the original one to user. So to deal with this some approaches to detect phishing consider capturing image of the page and convert it into text using optical character recognition (OCR) and uses the Google PageRank algorithm to find the top rank domains from search engines and compares them with the current page. Another study considers the textual clues from the DOM tree of the website to detect any anomalies in the DOM Objects. A file similarity is calculated between the targeted file and the suspicious web page so as to easily find out potential phishing web pages effectively.

4. Phishing detection based on other features

   Other features such as domain owner differs of an actual website and the fake website. As the phishing web pages are hosted on a less reputable domain and are usually taken down more frequently, this property can be used to decide whether the webpage given is phishing or not. A WHOIS Lookup is conducted to reveal the registrar given webpage and the registrar of the legitimate webpage . This is found using search engine analysis tools. Then these both domain owners are checked if the registrars for the suspicious and the legitimate website does not match then it is declared as phishing website.

Methodology

Our approach based on our related work considers the fundamental visual features of web pages and the registrar or the owner of the domain. The visual features i. e. CSS aren’t easily changed by the attacker as it may affect the appearance of the page and may alarm the user about the attack. The visual appearance of the web page is decided by the CSS rules applied to it. These CSS rules specify the visual properties of the web page elements.

The CSS rule consists of selector and a series of declarations that define the property value sets. For example: p {color: blue; font-size: 12px; }(1)

In the above example, ‘ p’ is the selector, color and font-size are the properties and blue & 12px are their respective values. In this way all the elements of the web pages and their CSS properties will be considered for building the influence vector. The attacker usually hides some elements and changes its CSS properties to display null or hidden, if such elements are detected in the suspicious webpage then we can say it is a phishing webpage.

As there are wo approaches of detecting phishing attacks using page-similarity, text content based and rendered page based. In the text based, keyword matching or sensitive text matching ratio are factors considered to detect phishing. However this can be evaded by replacing corresponding content using image and attackers may also add any invisible elements to the page. Rendered page based approach evaluates the rendered pages pixel by pixel. But this method will incur high performance cost.

To avoid the above problem we consider the web page’s layout structure. We extract the features in CSS file of the web page that influence the most of the visual appearance of the web page. These features are then converted into influence vector format to represent the static features of the page’s visual layout and then stored to find the similarity score between the legitimate web page and the suspicious one. The registrar of any particular domain is same throughout the whole website and the pages it consist of. A phishing page can be easily detected if the suspicious page’s owner doesn’t match with the owner of the original legitimate web page. The owner's name can be retrieved by performing WHOIS lookup. The main reason to use the WHOIS information is because many legitimate websites have different domain name for their secure web pages. So the other one used may be detected as a phishing page. Thus considering the similarity score and the similarity of registered owner of the suspicious web page and legitimate web page a phishing page will be detected. The similarity score calculated of both the web pages will be compared against a preset threshold value. If the similarity score is more than the threshold value then the web page is considered to be a phishing web page and if the owners of both the web pages don't match then also the suspicious page will be considered as a phishing web page. Considering these both factors will ensure that we detect the phishing attacks more accurately.

Evaluation and Analysis

In this section we evaluate and analyze the two methodologies we will be using for our project the Phishing Alarm. Of the two methodologies one is using the fundamental visual characteristics i. e. CSS and the other is based on the domain owner name.

In the method using visual characteristics, a large data set of 9, 307 verified phishing websites was collected by Jian Mao et al. from phishtank. com. The similarity values of the phishing pages when compared with their target pages is 0. 8 for 66. 91% and less than 1% have their similarity score below 0. 1. The suspicious web pages and the non-targeted web page's similarity score is calculated, 99. 44% of have a score below 0. 1.

This data is used to set the threshold value which is set as 0. 1 as it gives the best true positive rate and the true negative rate. Three basic metrics, precision, recall and F1-measure are used to describe the detection performance. For this 289 valid phishing web pages from evaluation set were used and 283 out of 289 web pages were correctly identified as Phishing pages. While from 246 legitimate web pages none of them was classified as Phishing web page. So it gives 0% false positive rate.

A dataset of 167 phishing pages and 51 legitimate web pages was collected by Choon Lin et al. to detect phishing attack by matching the domain name's owners. The domain registrar is obtained by using open source GNU-whois for Win32 application. The true positives obtained by matching the owner name is 98. 20% and the false positive rate is as low as 5. 88%. The overall results are given below:[image: image5. png][image: image6. png]Fig. 5. Registrar based phishing detection result.

Conclusion

Currently phishing is the most popular attack causing great economic loss to its victim. The most challenging task in this domain is to implement a system that can counter dynamically changing phishing strategies of the attacker. In this paper we have proposed a robust phishing detection approach called phishing alarm that checks the CSS based features, page similarity features and domain owner of the suspicious web page with the benign webpage and calculates its threshold value. The results using both this approaches individually have given a great performance of detecting 97. 92% of phishing websites using visual Characteristics and giving a 98. 20% true positive rate when used domain owner name similarity approach. Thus a combination of these two approaches would help us get better results and thus increase the efficiency as well as accuracy of our approach to detect the malicious phishing pages and alarm the user before visiting them. Phishing alarm will be prototyped as a Google Chrome extension for protecting users from visiting such phishing websites and falling prey to cybercrime.

Acknowledgment We are grateful to the Information Technology department for providing us guidance and resources throughout the project survey. We would like to extend our special thanks our guide Prof. Martina Rodrigues.