Expert Systems With Applications 53 (2016) 231–242

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

New rule-based phishing detection method

Mahmood Moghimi, Ali Yazdian Varjani*

Faculty of Electrical and Computer Engineering, Tarbiat Modares University, Jalal Ale Ahmad Highway, Tehran 14115-111, Iran

ARTICLE INFO

Keywords:
Phishing
Internet banking
Classification
SVM
Sensitivity analysis
Browser extension
Rule-based

ABSTRACT

In this paper, we present a new rule-based method to detect phishing attacks in internet banking. Our rule-based method used two novel feature sets, which have been proposed to determine the webpage identity. Our proposed feature sets include four features to evaluate the page resources identity, and four features to identify the access protocol of page resource elements. We used approximate string matching algorithms to determine the relationship between the content and the URL of a page in our first proposed feature set. Our proposed features are independent from third-party services such as search engines result and/or web browser history. We employed support vector machine (SVM) algorithm to classify webpages. Our experiments indicate that the proposed model can detect phishing pages in internet banking with accuracy of 99.14% true positive and only 0.86% false negative alarm. Output of sensitivity analysis demonstrates the significant impact of our proposed features over traditional features. We extracted the hidden knowledge from the proposed SVM model by adopting a related method. We embedded the extracted rules into a browser extension named PhishDetector to make our proposed method more functional and easy to use. Evaluating of the implemented browser extension indicates that it can detect phishing attacks in internet banking with high accuracy and reliability. PhishDetector can detect zero-day phishing attacks too.

1. Introduction

Over the past few years, following the growth of communication networks, internet as the biggest has been widespread popular. Using anonymity provided by the internet, hustlers set out to deceive people with false offers and make themselves look legitimate in this medium (Arun et al., 2012). With increased terminals for access to information, internet banking creates the need for using reliable methods in order to control and use confidential and vital information. Today, financial crimes are transformed from direct attacks into indirect attacks. In other words, instead of bank robbery, criminals try to target bank's clients with a specific trick (Vrîncianu & Popa, 2010). Attacks on computer security are classified in three types: physical attacks, synthetic attacks, and semantic attacks (He et al., 2011). Phishing is one of the types of semantic attacks. In these types of attacks, vulnerabilities in the users are targeted; for example, the way users interpret computer messages (He et al., 2011), because most of the users read information sources without verifying them, and respond their demands.

Generally speaking, phishing is a kind of electronic identity theft in which a combination of social engineering and fake website creating methods is used to deceive user to disclose his/her confidential and invaluable details (Aburrous, Hossain, & Dahal, 2010). Most phishing attacks start with an electronic letter which claiming that has issued by a reputable company. This email encourages the user to click on the address that is provides in its content. This address directs the user to an illegal webpage, which is designed similar to a valid website, e.g. the site of a bank or a financial institution. According to report of Anti-Phishing Work Group (APWG) which is a non-profit organization working to provide anti-phishing education to enhance the public understanding of security, more than 66% of phishing attacks target financial institutions and online payment systems (Cassidy, 2013) (Fig. 1). In addition, most of the phishing attacks made through hacked web servers. According to this report, in September 2012, the United States of America's phishing was the host of more than 73% of websites (Cassidy, 2013).

To date, different methods have been proposed in order to detect phishing attacks. According to APWG, generally the defense mechanisms against phishing attacks are divided into three groups: identification methods, prevention methods, and modification methods (Abu-Nimeh, Nappa, Wang, & Nair, 2007). To identify and prevent from these types of attacks, different approaches are

* Corresponding author. Tel.: +98 2182883398
E-mail addresses: m.moghimi@modares.ac.ir (M. Moghimi), yazdian@modares.ac.ir (A.Y. Varjani).

http://dx.doi.org/10.1016/j.eswa.2016.01.028
0957-4174/

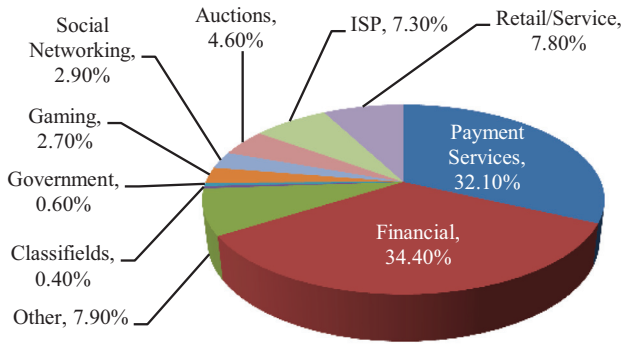

Fig. 1. Different industries affected by phishing in 2012 (Cassidy, 2013).

used whether in an email or in a website. We categorize these approaches into four groups:

- Black list/White list,
- URL evaluation,
- Visual assessment/Content evaluation,
- Hybrid approaches

Numerous tools are designed using white list or black list approach. Most of these tools authorize or reject a website through one or more references. Weakness of this approach is the lack of scalability and the ability to update the references quickly (Abu-Nimeh et al., 2007). Since creating websites often is cheap and easy, and their average life span may be a few hours, this approach in itself has low efficiency in prevention from these types of attacks (Aburrous et al., 2010). On the contrary, evaluating of apparent characteristic of webpage or its web address, is one of the best and simplest ways for phishing attacks detection, on which many studies have been conducted (Abu-Nimeh et al., 2007; Aburrous et al., 2010; Alkhozae & Batarfi, 2011; Arade, Bhaskar, & Kamat, 2011; ALmomani et al., 2012; Huang, Qian, & Wang, 2012; Rami, Thabtah, & McCluskey, 2014). In this approach, authors attempt to identify phishing attacks through analyzing website's information such as site logo, webpage visual similarity, security issues, and other web page characteristics (Alkhozae & Batarfi, 2011).

In this paper, we use this general approach to present a new rule-based method to detect phishing attacks on internet banking websites. Our method is based on novel feature sets, which determine the relationship between the content and the URL of a page. We used approximate string matching algorithms to compare address of each page resource element with the webpage URL. We also take consideration on how these resource elements load in a webpage; do they load from secure address or not? Our proposed feature sets include four features to evaluate the page resource identity, and four features to identify the access protocol of page resource elements. We used Support Vector Machine (SVM) algorithm to classify and detect phishing pages. We employ a related method to extract the hidden knowledge from our classification model. Finally, we implement our rule-based method in form of a browser extension called PhishDetector, which has a high accuracy in detection such attacks in our experimental results. The proposed method is independent of third-party services such as search engines or web browser history. Our main research contributions are summarized as follows:

- We proposed two novel feature sets to increase the accuracy of webpage classification.
- Proposed features are extracted from webpage content and they do not have any dependency to search engines, browser history and/or black/white lists.
- Since the proposed features extracted from page content, they are language-independent too.
- To make future development easy, we proposed a rule-based system by extracting the hidden knowledge from our classification model.
- We provide an easy to use chrome extension from our proposed rule-based method to detect phishing attacks on internet-banking websites.
- Our presented rule-based method can detect zero-day phishing attacks with high accuracy.

The rest of the paper is organized as follows: The next section reviews related works. Section 3 describes the proposed method and proposed features in detail and the way of the features vector made. Section 4 describes the data preparation for evaluation. In section 5, the method evaluated by real data includes phishing and legitimate websites. Limitation of our study discussed in section 6, while conclusion and future works discussed in section 7.

2. Related works

In 2010, Aburrous et al., provided an intelligent system to detect phishing pages in e-banking (Aburrous, Hossain, Thabatah, & Dahal, 2010). Their model is based on fuzzy logic combined with data mining algorithms to characterize the e-banking phishing website factors and to investigate its techniques by classifying the phishing types (Aburrous et al., 2010). Their approach was to apply fuzzy logic and data mining algorithms to assess e-banking phishing website risk on independent 27 characteristics and factors of a forged website. They got 86.38% classification accuracy with 10-fold cross-validation, which is relatively considered low. They also did not mention how they extract the 27 features for a webpage.

In the study carried out by He et al., they provided a system based on page content, HTTP transaction, and search engine results, which could identify phishing pages with an accuracy of 97% (He et al., 2011). In that study, the method was mainly based on CANTINA (Xiang, Hong, Rose, & Cranor, 2011), anomaly based web phishing page detection and with several additions and modifications (He et al., 2011). SVM algorithm also was used in order to classifying the output. The key feature used in the above study and other studies similar to Zhang et al. (Xiang et al., 2011), is the direct effect of the search engines ranking in page classification. If a webpage has high ranking in search engines, it will be considered as a legitimate website. In such cases, the attacker may use search engine poisoning techniques in order to increase the ranking of a forged website and index it legitimately (Gaurav, Mishra, & Jain, 2012).

By Arade et al., 2011, the authors used a new algorithm for approximate string matching in order to compare the webpage address and the addresses in the database of the proposed system. In the aforementioned algorithm, two strings are divided into a series of two-letter strings and then they will be compared with each other. If the similarity is more than 60%, the webpage will be considered as a legitimate otherwise, the webpage content will be checked and the aforementioned algorithm will run for all webpage links. The problem presented in this study is the probability of occurring false positive incidence. Thus, legitimate webpages may consider as phishing. Same feature used by Xiang et al., 2011, which may cause to produce false alarm. This lack of similarity existing between page resources address and page address (URL), has been used in related studies as an index to distinguish a valid site from a fake one (He et al., 2011; Xiang et al., 2011). In our study, we used this concept for all individual page resource elements (Hyperlinks, Cascade Style Sheets, Images, and Script reference addresses) not only page hyperlinks. He et al., used a same approach in their study (He et al., 2011). They defined a feature named "*ID foreign requests*". They compare the domain with the URL identity and *term identity set*. Their approach is completely