Web Phishing Detection

ABSTRACT

A phishing attack is one of the most significant problems faced by online users because of its enormous effect on the online activities performed. In recent years, phishing attacks continue to escalate in frequency, severity and impact. Several solutions, using various methodologies, have been proposed in the literature to counter the web-phishing threats. Notwithstanding, the existing technology cannot detect the new phishing attacks accurately due to the insufficient integration of features of the text, image and frame in the evaluation process. The use of related features of images, frames and text of legitimate and non-legitimate websites and associated artificial intelligence algorithms to develop an integrated method to address these together. This paper presents an Adaptive Neuro-Fuzzy Inference System (ANFIS) based robust scheme using the integrated features of the text, images and frames for web-phishing detection and protection. The proposed solution achieves 98.3% accuracies. To our best knowledge, this is the first work that considers the best-integrated text, image and frame feature based solution for phishing detection scheme.

Introduction

Phishing is a form of social engineering attack in which an attacker attempts to fraudulently retrieve sensitive user information by sending an email claiming to be a legitimately established organisation. They scam the user into giving confidential information that could be used for identity theft (Arachchilage et al., 2016, Jakobsson and Myers, 2006). Commercial institutions and their end-users are regularly exposed to the threat of phishing attacks (Barraclough et al., 2013). The danger is continuing to grow due to an increase in deception, impersonation, fraud and multiple online attacks. Most attacks are delivered by an email luring users to click a link embedded in the email that takes them to a malicious website. The attackers usually target end-users'financial information by claiming to be their bank, a utility company, HM Revenue and Customs or other government agencies to persuade the end-user to open the document attached to the email, which then targets sensitive information on their system (Office for National Statistics, 2017). The main reason why phishing attacks are still successful is the lack of awareness and computer literacy among Internet users mostly with regards to Internet safety (Deshmukh et al., 2017). According to a report by the Anti-Phishing Working Group (APWG)1 , the total number of phishing websites observed in the fourth quarter of 2017 was 296,208. The most targeted sector is the payment service with 41.99 percent of phishing attacks, followed by software-as-a-service (SaaS)/webmail with 17.07 percent and financial institution with 15.48 percent (APWG, 2017). Currently, the increase in the use of computer devices such as smartphones and tablets for accessing information on the Internet has more significance in financial crimes both regarding direct and indirect attacks (Fatt et al., 2014). That is to say, robbing a bank has changed into deceiving Internet banking users by stealing their identities and fraudulently using them to gain access to their Internet banking account and take their money (Moghimi and Varjani, 2016). According to a Financial Fraud Action2 UK report for 2017, about £165 million lost to fraud related to Internet payment cards, remote banking and identity theft in 2017, and while this is 3.68% lower than the same period in 2016 (Financial Fraud Action, 2017). There is still a need to do more to protect

Internet users from phishers who want to steal their confidential information for financial gain (Khadir, 2015). Addressing this situation, Barraclough et al. (2013) proposed a robust model using neuro-fuzzy with few inputs. This model employs fuzzy logic in combination with a neural network. The purpose of using neuro-fuzzy is that it has universal approximation and the ability to use fuzzy if…then rules. Fuzzy logic performs well when dealing with the reasoning in high-level language information while neuro-fuzzy does well when dealing with raw data (Barraclough et al., 2013). Fuzzy logic is used to provide a mode of qualitative reasoning, which is closer to human decision making because it handles fuzziness and ambiguity by combining fuzzy fact and fuzzy relations. Hence, a neuro-fuzzy implementation helps a system to encode both unstructured and structured knowledge, while fuzzy rules enable the system to learn from examples (Stathacopoulou et al., 2005). In this paper, a scheme that uses an intelligent ANFIS algorithm with a knowledge model and one input is proposed. The ANFIS is a network structure method that facilitates systematic computation of gradient vectors, it combines the least-squares and the gradient descent methods, and it utilises a useful fusion learning technique to derive the output error (Çakıt and Karwowski, 2016). ANFIS is a model that uses various features inputs selection, and it trains the data with the least-squares application (Jang, 1996). The proposed intelligent system will combine a neural network and fuzzy logic (Arachchilage et al., 2016) with the capability of reasoning and learning through the knowledge model and external knowledge sources. This technique was chosen because it allows data learning by using the connectionist approach for computation, and therefore the exact rules are from the fuzzy inference point of view (Barraclough et al., 2013). The method in this study uses a table in which the features or data of a valid website are stored for reference purposes. The data will includes website images, text and frames features. A total of 35 features are extracted to model the ANFIS; 22 elements represent the structure of the text-based properties, eight features represent the framebased properties, and five elements constitute the image-based resources of the website. The focus of the proposed intelligent phishing detection and protection scheme is to hinder websitebased phishing attacks that aim to entice victims into giving out their confidential and sensitive information. The main contributions of this study are the use of hybrid website features such as frames, images and text to improve on previous works (Barraclough et al., 2013) based on text only. Hence, building a robust and thus accurate and vigorous classifier for intelligent phishing detection in online transactions using website properties to analyse and detect phishing. This study is significant because the proposed system will enable online users to have confidence in performing their web activities with peace of mind. The remainder of the paper is organised as follows: section 2 presents a review of the literature and related works. Section 3 describes the proposed intelligent system with the hybrid feature. Section 4 explains the extraction and analysis of website features. Section 5 covers the experimental procedure. Section 6 discusses the training and testing results. Section 7 concludes the paper by explaining this study's contribution to knowledge and outlining future work

Literature review

Phishing is a type of online fraud in which a scammer uses a website or email to dishonestly obtain confidential information such as credit card details and Internet banking passwords (Martin et al., 2011). Phishing websites constitute a severe problem due to the enormous effect on the financial and online retail sectors. Due to the recent advances in technology, various procedures can now be used in phishing attacks that enable attackers to masquerade as a legitimate entity. Hence, they trick users into entering their credentials, such as passwords, username and credit card details into a fake web page for the attackers' malicious use (Babu et al., 2010). Therefore, it is vital to prevent such attacks

and defend against website phishing attacks (Aburrous et al., 2008). Khadir and Sony (2015) reviewed different kinds of phishing detection techniques mainly focusing on linguistic techniques and machine learning technology in a study that covered works up to 2015. Their review highlighted that various anti-phishing toolbars had been developed to protect Internet users. One such example is the eBay toolbar that helps users to monitor the web pages the users visit and provides warnings in the form of a coloured tab on the toolbar (eBay, 2016). Another is SpoofGuard, a plug-in developed for Internet Explorer, which examines the web pages users visit and warns them as to whether a particular page is likely to be a spoofed site (Neil Chou, 2004, Barraclough et al., 2013). The use of non-executable files such as Microsoft Office and Adobe PDF documents attached to an email has been a component of many recent phishing attacks (Liao, 2008). Due to the failure of the filtering process of most email servers, antispam software and Internet mail clients, this type of attack has grown in popularity. Most email servers filter out any executable file attached to an email because of the risk they pose, but nonexecutable data can flow through and are considered safe by most users. Regrettably, a non-executable file constitutes a vulnerability that when exploited might allow a phisher to perform malicious actions on a victim's computer (Cohen et al., 2016).

The proposed intelligent phishing detection and protection scheme

we introduce the proposed intelligent phishing detection and protection system (IPDPS). We also look at the different issues that arise in detecting phishing websites. This section covers phishing detection implementation using sets of the dataset, the essential characteristics and features of phishing website extraction techniques. Developing with the anti-phishing methods, phishers use various phishing methods and more complex and hard-to-detect approaches. The most straightforward way for a phisher to swindle people is to make the phishing web page similar to their target. However, many distinctive and features can distinguish the original legitimate website from the clone phishing website like the spelling error, image alteration, long URL address and abnormal DNS records. The full list is revealed in Table 3 which is used later in our analysis and classification study. If an attacker clones a legitimate website as a whole or designed to look similar as they usually do in most attacks in recent times, our approach is that similar looking phishing web page content is not left for the users to check for the indicator or the authenticity attentively, but can detect by automated methods. Our approach is based on website phishing detection using the features of the site, content and their appearance. These properties are stored in a local database (Excel table) as a knowledge model and first compared with the newly loaded site at the time of loading against the dangerous web page offline. After the comparison was unable to detect the similarity, then the critical approach to compare the legitimate and fake using the features of the website with machine learning for an intelligent decision.

Features selection and detection criteria analysis

In this study, reviewing different phishing investigations, research papers, conducting a separate phishing experimental case study give us more insight into the selection of the feature used for our phishing classification. Given this, we can extract 35 elements and factors which characterise the signature of any phishing website incident. These datasets divided into seven criteria that are

distributed into three layers, depending on the attack type. The most popular feature selection methods in the literature are ChiSquare (x 2) and information gain. Chi-Square is the commonly used method and adopted in this study; evaluated features are by computing Chi-Square statistics on classes (Gaunt, 2016). The information gain technique is also used in feature selection, which decreases the size of features by calculating the value of each attribute and ranking them. In other words, information gain selects elements through scores (Zeng et al., 2016). In this approach, a subset of initially chosen features is only used for testing and training the classifier (Abunadi et al., 2013). Feature extraction usually converts the original feature space into a more compact space. However, the original features are retained and transformed into a new reduced space with only a few representative sets (Zareapoor and Seeja, 2015). This approach mainly uses principal component analysis (PCA) and latent semantic analysis (LSA). Principal component analysis reduces the dimension of the data by transforming the actual attribute space into a smaller one (Vidal et al., 2016). That could achieve by converting the real variables Y = [y1, y2, … , yn] (where n is n tan h number of actual variables) into new variables, T = [t1,t2, … ,tp] (where p is an n th number of the new set of variables). The LSA technique is a novel-based method of text classification. The approach analyses the relationship between a concept and term contained in unstructured data, and it has the ability to correlate semantically related value that are latent in nature (Marcolin and Becker, 2016). These processes are used to convert the hybrid features into data that can be used to train and test our model.

Conclusion and future work

This paper presented an intelligent phishing detection and protection scheme by employing a new approach using the integrated features of images, frames and text of phishing websites. An efficient ANFIS algorithm was developed, tested and verified for phishing website detection and protection based on the schemes proposed in Aburrous et al. (2010) and Barraclough et al. (2015). A set of experiments was performed using 13,000 available datasets. The approach showed an accuracy of 98.3%, which so far, is the best-integrated solutions for web-phishing detection and protection. The primary contribution of this study is the integration of hybrid features that have been extracted from text, images and frames and that are then used to develop a robust ANFIS solution. Future work will include using another algorithm like deep-learning for phishing web page detection and compare the effectiveness with the current result. More also, a web browser plug-in will be developed based on an efficient algorithm to detect phishing website and thus protect users in real time.

Reference

Alkhozae, M. G. and Batarfi, O. A. (2011) 'Phishing websites detection based on phishing characteristics in the web page source code', International Journal of Information and Communication Technology Research, 1(6).

Abraham, A. (2005) 'Adaptation of fuzzy inference system using neural learning', Fuzzy systems engineering: Springer, pp. 53-83.

Abunadi, A., Akanbi, O. and Zainal, A. 'Feature extraction process: A phishing detection approach'. 13th International Conference on Intelligent Systems Design and Applications in Communications and Network Security (CNS) Bangi, Malaysia, 8-10 Dec. 2013: IEEE, 331-335.