ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Efforts and Methodologies used in Phishing Email Detection and Filtering : A Survey

Ripsa P Khadir
College of Engineering, Cherthala,
Managed by IHRD,
Established by the Government of Kerala, India

Sony P
College of Engineering, Cherthala,
Managed by IHRD,
Established by the Government of Kerala, India

Abstract: Rapid growth in technology has opened up wide means of communication. Electronic mail was a great contribution in the field of communication. Emails played the role of a valuable communication medium for all the internet users in the world. Phishing emails are spreading like an infectious disease nowadays. It results in economic losses and wastage of time of email users. Different kinds of phishing emails have been reported for this time. Many approaches have been developed in order to counteract this problem. In this paper, a model for phishing detection, which is based on the combination of linguistic techniques along with the machine learning technique is proposed. This paper also presents an overview of the main approaches developed with the aim of detecting and thereby filtering phishing emails and this work is done with the aid of a wide range of papers published in this field.

Keywords: Anti-phishing; Client side defenses; Machine Learning; Phishing; Server side defenses.

I. INTRODUCTION

The Internet is a universal network of computers, much of which is exposed to various electronic threats. Electronic mail is a vital communication medium among the internet users. Throughout its journey through the internet, the email is unprotected against various malicious attacks. Email-born attacks are expanding day by day, leading to economic losses as well as wastage of time to the users. Email phishing is a type of fraud which is intended to swindle victims for personal benefit or to intentionally harm through email. Spams also indicate a negative facet like the phishing emails. Spam is a junk or unwanted mail, which is annoying to the legitimate users, whereas phishing emails are illegal fraudulent schemes.

Phishing has become a common term associated with emails. The attackers use spam in order to accomplish their ultimate goals: either economic gain or mental satisfaction of damaging others. Phishing, also termed as brand spoofing is a kind of semantic attack that incorporates fake contents that replicates the real one. In this type of fraud activity, the victims receive emails that deceive them into providing sensitive and personal information such as account numbers, passwords or other personal to the attacker. It is actually a criminal mechanism which results in the theft of user's personal information and financial account credentials. It could be termed as email fraud. They take different forms like spoofing, bogus offers, requests for help, romance scam, Nigerian scam (419 scam) and lottery scam.

Stephen Hinde, the IS audit editor has outlined that in the year 2002, an economic loss of around $5 billion was due to Nigerian scams, famously known by the name 419 scam [1]. Anti-Phishing Work Group (APWG), that brings together the businesses affected by phishing attacks use to release reports on phishing. The APWG has released the latest, the phishing trends report for Q2, 2013. In addition to phishing websites, it studied on unique phishing emails, also termed as email campaigns [2]. APWG members reported that enlightened, focused content continues to make email a major attack target for phishing and hence phishing will continue to be a major issue for the internet users ahead [2].

Several approaches have been proposed in the last few years in order to overcome phishing. They can be categorized into two major sections: exhaustive anti-phishing efforts and methodologies and algorithms to detect and filter phishing. The former comprises the "human factor" which includes user awareness, social and psychological studies and the education of users and contributors. The latter presents different approaches and algorithms used to protect the user against phishing. Usually phishing attacks consist of two phases: distribution of malicious hyperlinks via unsolicited emails, and connecting to malicious hyperlinks by victims. Many approaches have been developed in the given two categories: client based and server based. Commercial proposals also exist for phishing email detection.

This paper is organized as follows: Section 2 details the exhaustive anti-phishing efforts. Section 3 elaborates the methodologies and algorithms used for phishing email detection and filtering. Finally, Section 4 presents the conclusion.

II. EXHAUSTIVE ANTI-PHISHING EFFORTS

The "human factor" also plays a major role in avoiding phishing to a great extent. It cannot be prevented by technical means alone always. Van der Merwe et al.[3] identified five crucial categories for users and organizations to consider in order to avoid phishing. They include education, preparation, avoidance, intervention and treatment [3]. The users must be aware of phishing and following points will contribute much to the same.

- The end users must be provided the knowledge about phishing and they should be able to identify phishing emails. Even some phishing emails can

give warnings that indicate that this email can be a scam.

- The after effects of phishing must be known in advance and must be prepared to face them with the appropriate measures. Different authentication mechanisms can be employed in this scenario.
- The user must know how to avoid becoming a victim of a phishing attack. Different mechanisms like anti-spam filters and other commercial tools can be used for this purpose.
- The user will be the one who knowingly or unknowingly decides whether to make the phishing attack success eventually. Hence the user must be that much aware of the situation.
- The user may fall for the phishing attacks and may lead to identity theft and economic losses. After getting attacked, other measures that could be done are recovery purposes, contacting the appropriate organizations for keeping the personal information secure by other means [3].

A. User Awareness

Many studies have been conducted to analyze the behavior of users, their responses to the phishing emails and analyzed the results at different levels [4]. The study did not find any of these factors made a significant difference in the susceptibility of the user to the attack. Many users were not even able to find the phishing, even after knowing the chances of their presence. Individual users are the most vital element in an anti-phishing effort and they must take an active role to avoid becoming a victim of a phishing attack. Users can protect themselves and their personal information and credentials by following certain measures.

- Don't respond by sending personal and financial information. This occurs mostly when the user falls for phishing emails like lottery scams.
- Never click on embedded hyperlinks which may seem legitimate. Confirm it by typing the URL of the embedded link in the address bar of web browser.
- Never respond to an email indicating updating, validation , verification of bank accounts and also online payment services like paypal. The user must be aware that banks will not send such emails.
- Communicate directly with the organizations rather than responding to the mails.
- Check the hyperlinks embedded in emails rigorously. In hyperlinks, https: mostly indicates secure websites whereas http: indicates insecure ones.
- Check the financial account and credit card information directly.
- Information must not be entered in response to an email.
- Immediately report phishing attacks if found any, on the respective sites available for that purpose.

For the detection and filtering of phishing emails, one cannot trust themselves. In other words, user education alone would not completely provide an efficient solution to the problem.

III. METHODOLOGIES AND ALGORITHMS

Apart from user awareness strategy, many techniques and algorithms are developed to fight against phishing. Phishing filtering techniques are mainly classified into two types: client side techniques and server side techniques.

A. Client Side Defenses

The client side defenses for phishing are implemented on the browser side. The major browser-side methods are referred to as plug-ins. It warns the user on the spot of detecting a spoof website. It helps to improve the browser password management. Browser plug-ins are available for download. Anti-phishing software are a collection of programs. They are built with the aim of detecting phishing websites and emails. It is usually integrated along with the browsers as toolbars at the client side. In order to counter phishing, the main four commercial tools that are available are anti-virus, firewall, anti-spyware and anti-spam. Some of the other client side approaches are elaborated below:

a. Link Guard

Link Guard is an anti-phishing algorithm proposed by [5] and it is client based. It works by utilizing the generic characteristics of hyperlinks embedded within in phishing emails. After analyzing the embedded hyperlinks, they are classified into the following categories:

1. The category in which the destination DNS name does not match with the actual link.
2. In this category, the IP address is used directly in the URI or the anchor text in its place, instead of using the DNS name.
3. In this category, encoding schemes associated with the embedded links are considered.
4. The category in which the destination information is provided in its anchor text. The DNS name similar to the legitimate ones is used in the URI of the embedded links.
5. The unprotected nature of web sites targeted for the phishing attack are used by the attackers to fool the user [5].

The Link Guard algorithm is implemented at the user end. Link Guard is characteristics based and hence it can detect and prevent not only known phishing attacks but also unknown ones. It was implemented in Windows XP and includes two parts: a whook.dll dynamic library and a Link-Guard executive. This mechanism can detect up to 96% unknown phishing attacks in real-time.

b. Biometric Approach

This mechanism proposed by [6] is based on the biometric characteristics and it uses fingerprint recognition to authenticate users. It provides the end users a transparent process of signing and verifying email messages. The basic technique of this mechanism is enrolling a user fingerprint, then associating the fingerprint with a record that is unique to that user, and finally the user's fingerprint and unique record are used to authenticate the user, sign the user's email message, and thus verify other user's email messages. This mechanism, SEFR and is implemented as an email client. This technique offers secure email access; it helps to prevent email spoofing and man-in-the-middle attacks.

B. Server Side Mechanisms

Exhaustive anti-phishing efforts offers low cost to the user, but it must be delivered in a consistent manner where the user is not overloaded with information. Client side defenses can offer security only to a certain limit. Many approaches are developed at server side in order to detect and filter phishing emails. A discussion on some of the major approaches is listed in this section.

a. Agent Based Approach

Agent-Based approach is a distributed architecture proposed by [7] that resists different types of phishing attacks and it ensures online security. This approach presents a software framework which mainly focuses on a tab-nabbing attack. It is capable of perceiving and learning according to environmental changes as it is an agent-based approach. Instead of relying on end users, protection is more concentrated towards ISP. It uses the concept of flow analysis in order to ensure scalability and it is possible to analyze flow patterns and compare the network behavior of multiple sources. In this self-management architecture, data from real networks are used, followed by the analysis of the collected data using self-learning techniques and the bad neighborhood concept.

b. Separable Identity-Based Ring Signatures

Digitally-signed emails can be used in order to alleviate phishing attacks, provided the signatures should not destroy the traditional structure of an email, and a Public-Key Infrastructure must be acquired globally. Separable identity-based ring signatures are used in order to vanquish these hurdles. In this approach, put forward by [8], three systematic honest-verifier zero-knowledge (HVZK) proofs of knowledge of various pre-images of bilinear maps are presented. New identity-based identification (IBI) and signature (IBS) schemes are developed based on these proofs. A new IBI scheme based on bilinear maps is well organized and combined with the Waters IBE scheme resulting in a complete PKI-based system. Finally the first SIBR signature schemes, by transforming the new signature schemes and certain other signature schemes are constructed. Repudiability is offered in this mechanism due to the ring structure of these signatures. Along with identity-based public keys, a complete PKI are not needed. Ring constructions across different identity-based master key domains are offered by the separability feature. All together, the characteristics mentioned in this scheme make SIBR signatures a feasible solution to the email fraud problem.

c. An Anti-phishing Strategy Based on Visual Similarity Assessment

The visual characteristics are the basic idea behind this approach which is proposed by [9]. The idea is to identify possible phishing web sites, and evaluate wary page's similarity to actual sites listed by the system. It tracks emails on local mail servers at keyword and URL levels. Whenever a keyword requested by the user is found while monitoring, the details, including the legitimate ones are sent to the visual similarity assessment module. The features of the corresponding web pages are extracted and similarity measure is evaluated based on block-level, layout and style in the visual similarity assessment module. The evaluated value is compared against a threshold value and if it exceeds the threshold value, phishing report is issued.

d. DNS-based Email Sender Authentication Mechanisms

It is an email sender authentication mechanism proposed by [10]. SPF, DKIM and Sender-ID Framework (SIDF) are the three chief procedures used in this system. Among all the above mentioned mechanisms, a successful mechanism for certifying emails from a domain is furnished by DKIM. It overcomes the likelihood of false negatives. The DKIM approach does not allow unauthorized emails reach the user. The use of digital signatures by DKIM is different compared to that of by DNS and routing. This approach is not the best one since the emails that has passed the validation need not be a legitimate one and vice versa. The attackers can create genuine emails using their own domains. This mechanism does not offer a complete protection, but only a limited one. This approach is an untrustworthy one.

e. Machine Learning Based Approaches

This is the major category of phishing detection approaches. Different methods are developed in this area. These are termed as feature based approaches too. Detection of phishing emails can be done based on the structural features incorporated into the content. Based on that feature, different approaches are designed for detection and filtering of phishing emails. They include URL-based, script-based, keyword-based, behavioral-based and content-based. The different features include URL features, script features, keywords used, text block features, image block features and style features. Machine learning based approaches can be further subdivided into different sub-sections. Many approaches have been developed for phishing detection by using a bag of words model, based on different features, testing the performance of different classifiers, clustering methods, hybrid methods etc.

In the bag of words model based approach [11], the email dataset which is the input is illustrated as a disordered accumulation of words, ignoring the sequence of words and even syntax. It is based on classifiers and the classifiers include SVM, k-Nearest neighbor, Naive Bayes, Adaboost etc. The major snag is that this approach cannot deal with zero day phishing attacks. Many studies were conducted on comparing the performance of different classifiers. Abu Nimeh et al [12] has compared six classifiers namely Logistic Regression, CART, SVM, Neural Networks, BART and Random Forests and no standard classifier were found. Miyamoto et al. [13] also made a comparative study of machine learning algorithms for phishing detection. Ram Basnet [14] conducted the same using 16 features, but it gained low accuracy. Ganster et al. [15] compared between binary and ternary classification approaches by establishing 15 new online and offline features. But it took high cost because of online features.

Isredza Rahmi A Hamid et al. [16] proposed behavior-based features to detect phishing emails by observing the sender behavior. In this approach the behavior of senders

who tends to send email from more than a single domain and a domain that handle different kind of email sender domain is considered. The message-id field was also incorporated as a feature in this scheme. In this approach, the performance of different classifiers like Bayes Net, support vector machine (SVM), AdaBoost and Random Tree and it was found that Bayes Net and Random Tree achieved the highest accuracy and works well in distinct and small dataset.

An approach based on the relative probability of occurrence of the features was proposed by [17]. In this approach, about 18 features were used. The relative probability value was calculated for both the phish and ham training and test email datasets. Three stages are there in this approach: pre-processing, feature analysis and application of phishing detection using Feature Existence and Feature Decisive Value criteria (FEFDV). The appearance of a feature was indicated by binary value '1' and non-appearance by binary value '0'. Ham Decisive Value (HDV) Criteria and Phish Decisive Value (HDV) Criteria are applied in this approach for phishing detection [17].

A multi-stage mechanism was proposed by [18] which discovers named entities, which includes names of individuals, organizations, and locations; and hidden topics. This methodology adopted Conditional Random Field (CRF) and Latent Dirichlet Allocation (LDA) for operating on both phishing and ham email datasets. This approach employs natural language processing and machine learning. It is followed by the classification of each message as phishing or ham using AdaBoost. From the emails classified as phishing emails, the imitated entity is discovered using CRF. This mechanism detects phishing emails with no miss classification when the amount of phishing emails is less than 20%. The F-measure obtained was 100%.

A multilayer approach which works on the sequential implementation of three filters was proposed by [19]. The written content of emails is classified using a Bayesian filter, followed by the classification of non-syntactical content of emails with the aid of a filter that works based on rules. At last a filter based on an imitator of fake accesses, classifies the responses from the websites cited by hyperlinks embedded in the emails. Multi-tier classifications [20] is a serial procedural approach in which every tier, a different well known machine learning algorithm is used. This approach suggested three types of arrangements for the classifiers c1 (SVM), c2 (Adaboost) and c3 (Naive Bayes). It got about 97% accuracy for the arrangements c1-c2-c3 and c1-c3-c2. It got the least accuracy of about 93.33% in the arrangement c2-c3-c1. However, this technique requires more time for its execution. This approach also faces complication in its analysis as there are multiple stages to be passed in order to get the final result.

PHONEY: mimicking the user response was proposed as a novel approach by [21]. This technique uses dummy responses which mimic the genuine users. It works by reversing the character of the victim and the attacker. In this methodology, the email contents with embedded hyperlinks are analyzed. Then the content scanner will receive the web page for analysis, then, extracts the data from the Web page. The results are then compared against the values in the hash database, thereby classifying emails into phishing or non-phishing.

IV. PROPOSED MODEL

Machine learning approaches are found to be the most promising methodology in the detection and filtering of phishing emails. The current approaches have limitations in terms of their accuracies and performances. In [22], it was proved that combining linguistic techniques along with the machine learning technique can extract high quality noun phrases. They used the extracted noun phrases for summarizing the email messages. They also suggested that the use of a combination of classifiers will improve the accuracy compared to that of using machine learning technique alone.

We propose a model inspired by these results. The model is shown in Figure.1. The system model incorporates the process of HTML parsing in order to extract the content of the emails. It uses the linguistic techniques to extract named entities, that is noun phrases and also in the process of relationship extraction between entities.

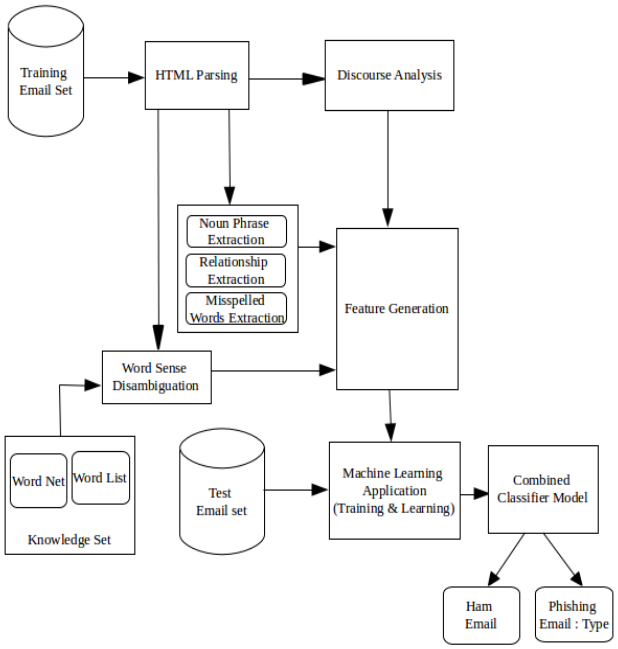

Figure.1. Proposed Architecture

In order to solve lexical ambiguity, we employ word sense disambiguation. Discourse analysis is employed in order to interpret the content of emails. This will give us the summarization of email messages and helps to identify the type of the scam by looking after the summarized form of email messages. For each type of scam, the features are selected. Forwarding the results towards the machine learning technique is the next step in this model. In the proposed system, we would like to use a combination of classifiers. We have selected the classifiers SVM and Naive Bayes for the purpose. This strategy will improve the accuracy of the overall system. Machine learning approaches are like a deep ocean in the field of phishing detection. They are one of the most promising approaches.

V. CONCLUSION

Phishing emails get enormous day by day and they are annoying and dangerous to legitimate internet users. Economic losses due to phishing emails are increasing in a nonstop manner. Different kinds of phishing attacks are emerging per year. Attackers are developing new types of attacking methodologies overcoming the prevention and filtering mechanisms employed currently. In this paper, many approaches for phishing email detection and filtering has been organized based on a wide range of papers. Different techniques were discussed and server side implementations were found more efficient and out of that learning based approaches were the most promising one. Still, it has the limitations in terms of accuracy and performance.

We propose a methodology incorporating linguistic features along with machine learning for phishing email detection and filtering. It can lead to even more promising results. This approach has already been used in the email summarization process. The current phishing filtering mechanisms are static and they are not fully efficient. Hence it raises the need for the development of efficient phishing detection and filtering mechanisms in every aspect.

VI. REFERENCES

[1] Stephen Hinde: Spam, scams, chains, hoaxes and other junk mail, 0167-4048/02US, Elsevier Science Ltd(2002).

[2] Anti-Phishing Work Group: Phishing Activity Trends Report 1st Quarter(2013), http://www.apwg.org

[3] Merwe A.v.d., Looc M., Dabrowski M., "Characteristics and responsibilities involved in a Phishing attack", in: Proc. of the 4th International Symposium on Information and Communication Technologies, Trinity College Dublin, pp. 249–254, Cape Town, South Africa(2005).

[4] Dhamija R., Tygar J.D., Hearst M., "Why phishing works", in: CHI 2006, April 22–27(2006).

[5] Juan Chen, Chuanxiong Guo : "Online Detection Prevention of Phishing Attacks (Invited Paper)", IEEE(2006).

[6] A.S. Zadgaonkar, Suresh Kashyap, Murari Chandra Patel : "Developing a Model to Detect E-mail Address Spoofing using Biometrics Technique", International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-6, May(2013)

[7] Sarika S, Dr.Varghese Paul : "Distributed Software agents for antiphishing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, May(2013).

[8] Ben Adida, Susan Hohenberger, Ronald L. Rivest : "Separable Identity-Based Ring Signatures: Theoretical Foundations For Fighting Phishing Attacks", Computer Science and Artifical Intelligence Laboratory; Massachusetts Institute of Technology; 32 Vassar Street; Cambridge, February 28(2005).

[9] Wenyin Liu, Xiaotie Deng, Guanglin Huang, Anthony Y. Fu An "Antiphishing : Strategy Based on Visual Similarity Assessment", IEEE Computer Society(2006).

[10] Amir Herzberg : "DNS-based email sender authentication mechanisms: A critical review", Israel computers & security 28, pp. 731–742(2009)

[11] Blanzieri, EnricoBryl, Anton, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, Springer Netherlands, vol. 29,no.1, pp. 63-92(2008).

[12] S. Abu-Nimeh, et al. : "Distributed phishing detection by applying variable selection using Bayesian additive regression trees", In : IEEE International Conference on Communications,vol.1, pp. 1-5(2009).

[13] D. Miyamoto, et al. :" An evaluation of machine learning-based methods for detection of phishing sites", Advances in Neuro-Information Processing,vol.1, pp. 539-546(2009).

[14] S. M. Ram Basnet, and Andrew H. Sung :" Detection of Phishing Attacks: A Machine Learning Approach", Studies in Fuzziness and Soft Computing, springer, vol. 226, pp. 373-383(2008).

[15] W. N. Gansterer, et al. : "E-Mail Classification for Phishing Defense", In : Proc. 31th European Conference on IR Research on Advances in Information Retrieval, Springer Conf, Toulouse, France, pp.449-460(2009).

[16] Isredza Rahmi A Hamid, Jemal Abawajy, Tai-hoon Kim : "Using Feature Selection and Classification Scheme for Automating Phishing Email Detection", Studies in Informatics and Control, Vol. 22, No. 1, March(2013).

[17] Noor Ghazi M. Jameel, Loay E. George : "Detection Phishing Emails Using Features Decisive Values", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 7, July(2013).

[18] Venkatesh Ramanathan, Harry Wechsler : "Phishing detection and impersonated entity discovery using Conditional Random Field and Latent Dirichlet Allocation", Computers & security34(2013).

[19] M Dolores del Castillo, Angel Iglesias, and J Ignacio Serrano, H Yin et al. : "Detecting Phishing E-mails by Heterogeneous Classification", IDEAL 2007, LNCS 4881, pp. 296–305(2007).

[20] Rafiqul Islam , Jemal Abawajy :" A multi-tier phishing detection and filtering approach", Journal of Network and Computer Applications 36, pp. 324–335(2013).

[21] Madhusudhanan Chandrasekaran, Ramkumar Chinchani, Shambhu Upadhyaya : "PHONEY: Mimicking User Response to Detect Phishing Attacks", In : Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks IEEE(2006).

[22] Smaranda Muresan, Evelyne Tzoukermann, Judith L Klavans : "Combining Linguistic and Machine Learning Techniques for Email Summarization", In : proceeding ConLL '01' proceedings of the 2001 workshop on Computational Natural Language Learning- Volume 7, Article No. 19(2001).