A Study On: Implementation of ML(Machine Learning) in Compromised Emails

Riya Bhadra,
Graduate,
Department of Computer Science and Engineering,
Presidency University, Bangalore.

Kokila S,
Assistant Professor,
Department of Computer Science and Engineering,
Presidency University, Bangalore.

Abstract

The aim of this study is to give a novel tool for finding out phishing attacks and finding solutions to counteract such threats. In the following article we tell about the process of how to develop a scrum-based implementation of algorithms for Neural Networks, Automatic Learning, and Feature Selection. This tool has the ability to find out and mitigate a phishing attack found inside the e-mail server. For the validating the obtained results, we have used the information of blacklist of Phish Tank, which is a collaborative cleansing house for details about phishing on the net. The concluded proof of concept showed that the implemented feature selection algorithm discards the not useful characteristics of mail and, that the neural network algorithm takes up these characteristics, establishing an optimal level of learning without unnecessary stuff. It also tells about the functionality of the solution proposed.

Keywords*— Feature Selection, Phishing, Security, Social Engineering, Neural Networks.*

INTRODUCTION-

According to [1] Social Engineering's principle is based on the fact that, users seemingly are the biggest weakness around their security in any system. It is also based on the organic tendency of people to react predictably in certain situations. That's how an attacker effortlessly takes advantage of this organic tendency – as in when we give our finance related details to any bank officer - instead of trying to find security faults in computer systems. The attack of identity theft in commercial transactions known as Phishing [2]. It is one of the Social Engineering techniques with the strongest influence. It is denoted by trying to acquire confidential information deceptively. This technique has been used by criminals(cyber).

For such cases, several studies have been analysed [3]–[7] where different automatic learning algorithms have been compared and in which all the proposals have been exposed. Attacks of these types will continue to appear with increasing complexity and with a higher frequency.

In this study, we aim to identify and stop phishing spoiled e-mails. For achieving this, Neural Networks and Feature Selection techniques were merged, which helped to find out the probability of Phishing type e-mail. As a proof of this concept, three datasets were used for implementation of the algorithm, which were compiled in course of nine months from public email lists obtained from Debian, and executed to be analysed in a virtual environment. Every email was compared with black Phishing lists received from Phish Tank, in order to distinguish between Phishing and HAM (non-Phishing emails). The main give away from this study has been designing and implementing a less expensive counter-measure, finding out and mitigating phishing attacks, which are already stored in corporate e-mail server, using automatic learning methods.

The remainder of the article is in the following order: in Section II we discuss the architecture of the system used, methodologies and techniques. In section III we validate and analyse the found out results with our proposal. Finally, section IV showcase the inferences and future work lines.

METHODOLOGIES-

A. Process of Design

According to (Trigas, 2012) [8], "Scrum looks as a method aimed at products that are technological, which is based on the idea of making small development cycles named as Sprints or iterations". The Scrum consists of a variety of steps like: (i) Choosing requirements; (ii) Planning the task; (iii) Sprint being executed; (iv)

Meetings held monthly; (v) Meetings held daily;(vi) Delivery. The methodology gives for each activity the time and manner of execution, the personnel involved. The prototype is illustrated in Fig. 1.

1) *Architectural diagram:* As stated to [9], an architectural diagram proposes the complete view of the system that is be built, as it showcases the architecture and organization of the components of software. Fig. 1 showcases the proposed architecture of the system, where reading, browsing, mitigating detecting, and alerting of threats of Phishing as mentioned below. When a new email is obtained on the server, mail client receives it after that from the server and then the mail is subsequently processed in the MatLab software. The mail's characteristics are extracted in the software for being executed by the Feature Selection algorithm. The learning vector is generated with help of the Neural Networks algorithm after the selection of characteristics, hereby finding out whether it is HAM (mail without Phishing) or Phishing mail. The email is stored in a blacklist in a MySQL database if it is found that Phishing exists.

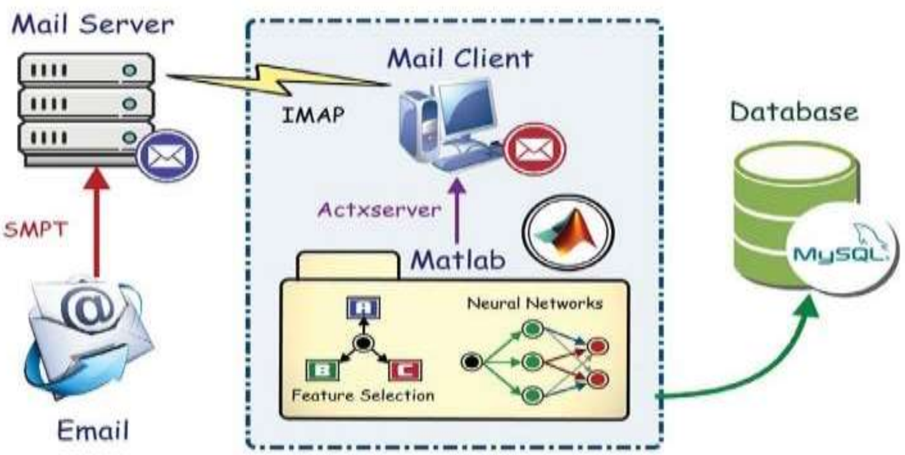
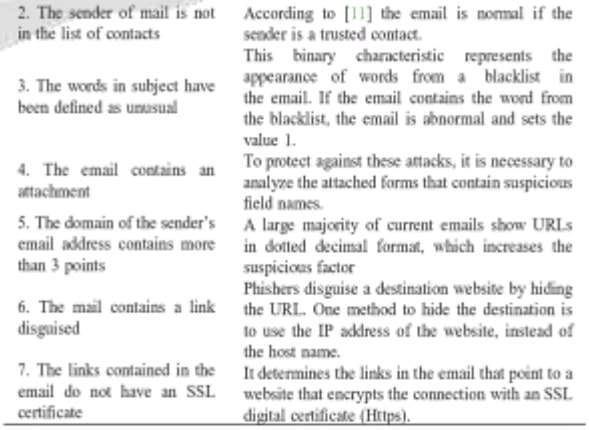


Fig. 1: Architectural diagram(proposed)

B. Development Process

The method used here is Feature Selection, pre-processing of the characteristics of the electronic mails are allowed and the removal of not so necessary ones are also allowed. Along with that Neural Networks are used for constructing the machine learning vector. Fig. 2 illustrates the given application's flow diagram.

TABLE I: Description of features



1.Mail has image [10] represents appearance of links	This binary feature proposed by with external link. in emails presenting images with the objective of detecting obfuscated URLs.
2. The sender of mail is not in the list of contacts	According to [11] the email is normal if the sender is a trusted contact.
3. The words in subject have been defined as unusual	This binary characteristic represents the appearance of words from a blacklist in the email. If the email contains the word from the blacklist, the email is abnormal and sets the value 1.
4. The email contains an attachment	To protect against these attacks, it is necessary to analyze the attached forms that contain suspicious field names.
5. The domain of the sender's email address contains more than 3 points	A large majority of current emails show URLs in dotted decimal format, which increases the suspicious factor
6. The mail contains a link disguised	Phishers disguise a destination website by hiding the URL. One method to hide the destination is to use the IP address of the website, instead of the host name.
7. The links contained in the email do not have an SSL certificate	It determines the links in the email that point to a website that encrypts the connection with an SSL digital certificate (Https).

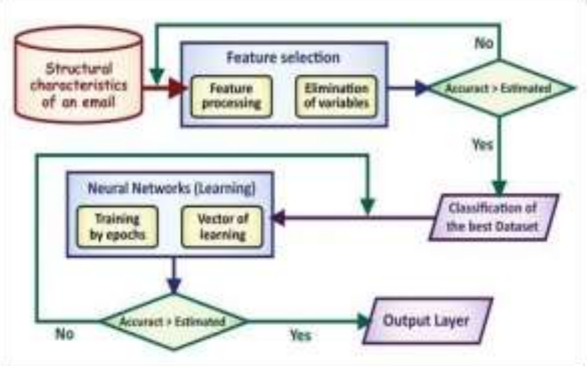


Fig. 2: Mitigation model and Phishing Detection flowchart

1) Feature Selection Algorithm: Phishing is the practise of using bogus websites and emails that look legitimate to deceive a potential victim into disclosing sensitive personal information. In light of these circumstances, phishing attacks were created, simulating the transmission of emails based on the characteristics of the email, which are detailed in Table I.

2) Neural Networks Algorithm: A reduced data set is produced from these features once the key traits have been extracted via feature selection. We trained the network and classified the data using this collection of data. As we moved forward with the data classification, we also established the required inputs for creating the neural network learning model. The distribution of these has been balanced between examples that are both good and negative.

3) Application combining Feature Selection and Neural Networks: The software needed to connect to the mail client was created after the predictive model was created. The two algorithms have been integrated to do this task, defining a main class in the process.

4) Attack mitigation: There is a need to neutralise a phishing attack after it has been discovered. The approach used has been to move the email that was identified as a threat to a quarantine directory and revoke the user's access to it. Before beginning the procedure, the user is informed. The message is transferred to the quarantine directory after the user is informed. All emails that have been flagged as threats are kept in this database and can be found using their ID.

RESULT EVALUATION-

A .Tests and performance analysis

The blacklist maintained by PhishTank was the information source used to validate the results. In addition, the experimental configuration began with the collection of emails from the website Mailing Lists Debian, 2019 by signing up for the many lists it offers. A local server was used to hold these emails, which came to about three thousand in total. These emails were divided into three equal-sized data sets, which were then arranged according to the following time frames: (1) January to March; (2) April to June; and (3) July to September. The number of emails that contained phishing as determined by the blacklist classification is shown in Fig. 3, where we assessed the URLs flagged as phishing. Since 179 Phishing emails were obtained over the course of the three time periods, the percentage of Phishing in each data set in this classification is very low. This amounts to 5.96% of the 3000 emails that were analysed in total.

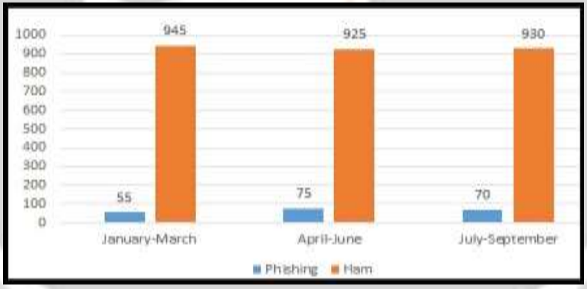


Fig. 3: Data set returned with the blacklist analysis

The outcomes following the execution of the suggested software are shown in Figure 4. Given that a total of 204 Phishing emails have been encountered as opposed to the 179 emails returned by the blacklist, there is not much of a change from the prior figures.

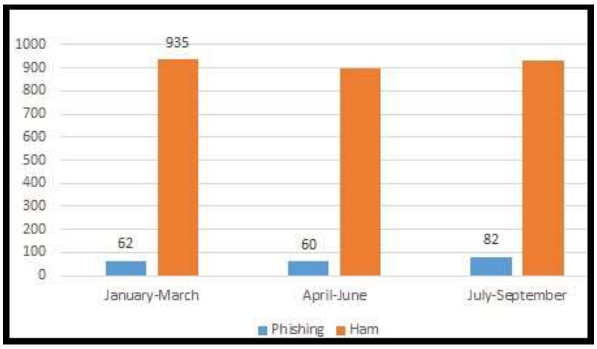


Fig. 4: Data set returned by the software proposed

Table II shows the software's output, with the first data set yielding about 92.9% efficacy, the second about 91.2%, and the third about 97.3%. It should be mentioned that the algorithm has a maximum margin of error of about 8.8% and a minimum of about 2.7% for correctly identifying emails that have been compromised by phishing.

TABLE II: Efficiency of the model

	Accuracy	Precision	Error	Recall
1	0.929	0.983	0.071	0.873
2	0.912	0.981	0.088	0.840
3	0.973	0.974	0.027	0.971

INFERENCE AND FUTURE WORK –

This study showed that it is possible to identify phishing by the correct identification and use of an email's structural attributes, enabling a more in-depth investigation of the technical material that phishers employ to commit crimes. The requested software tool has been implemented using the Agile Scrum approach. Additionally, the automatic learning, feature selection, and neural network algorithms have all been implemented with the help of the Matlab process tool. Due to the fact that the implemented methods complement one another during detection, the results of the concept tests are highly encouraging. An average accuracy of 93.9% was obtained when the findings from the three data sets were evaluated. It also demonstrates how well the suggested approach works. We intend to build a solution using deep learning and Bayesian neural networks in future work.

REFERENCES:

[1] J. Mieres. (). Ataques informa´ticos. debilidades de seguridad comu´nmente explotadas. 2009.

[2] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, “A comparison of machine learning techniques for phishing detection,” in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, ACM, 2007, pp. 60–69.

[3] S. Gastellier-Prevost, G. Granadillo, and M. Laurent, “Decisive heuristics to differentiate legitimate from phishing sites,” Jun. 2011, pp. 1–9.

[4] A. Martin, N. B. Anutthamaa, M. Sathyavathy, M. M. S. Francois, and V. P. Venkatesan, “A framework for predicting phishing websites using neural networks,” *CoRR*, vol. abs/1109.1074, 2011.

[5] M. Aburrous, M. Hossain, K. Dahal, and F. Thabtah, “Intelligent phishing detection system for e-banking using fuzzy data mining,”

Expert Systems with Applications, vol. 37, no. 12, pp. 7913–7921, 2010, ISSN: 0957-4174.

[6] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, “A comparison of machine learning techniques for phishing detection,” in *Proc. of the Anti-phishing Working Groups 2Nd Annual eCrime*, ser. eCrime ’07, Pittsburgh, USA: ACM, 2007, pp. 60–69.

[7] A. Hamid, I. Rahmi, J. Abawajy, and T.-h. Kim, “Using feature selection and classification scheme for automating phishing email detection,” *Studies in Informatics and Control*, vol. 22, pp. 61–70, Mar. 2013.

[8] M. Trigas. (). Metodolog´ıa scrum. July 2012.

[9] Y. Li and S. Manoharan, “A performance comparison of sql and nosql databases,” in *2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, Aug. 2013, pp. 15–19.

[10] W. N. Gansterer and D. Po¨lz, “E-mail classification for phishing defense,” in *Advances in Information Retrieval*, M. Boughanem, C. Berrut, J. Mothe, and C. Soule- Dupuy, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 449–460.

[11] F. Toolan and J. Carthy, “Feature selection for spam and phishing detection,” in *2010 eCrime Researchers Summit*, Oct. 2010, pp. 1–12.