Deep Learning based Detection of DNS Spoofing Attack

Mykola Kozlenko, Valerii Tkachuk

Department of Information Technology
Vasyl Stefanyk Precarpathian National University
Ivano-Frankivsk, Ukraine

***Abstract*—In this paper, we propose to use a classification model based on an artificial recurrent neural network (RNN) and a deep learning approach for DNS spoofing detection. It is proposed to use DNS data as well as TCP header and IP header data as features of the detection model. Using of IP header data, particularly, such feature as hop count is well known and widely used for IP spoofing. The main challenge is to apply these approaches to DNS spoofing detection. The aim of the research is to proof the feasibility of the proposed technique and to obtain metric values. The methodology of the research is to evaluate the deep learning model trained on the artificially synthesized dataset. The numerical results from simulations are used to evaluate the performance. The paper reports the accuracy about 70%.**

Keywords—deep learning, spoofing attack, network security, DNS, TCP, IP, RNN.

I. Introduction

Domain Name Server (DNS) is a critical component of the operation of Internet applications. It provides a way to resolve domain names to their corresponding IP addresses. DNS spoofing also referred to as DNS cache poisoning is an attack in which altered DNS records are used to redirect online traffic to a fraudulent resource that possibly resembles its intended destination. This results in traffic being diverted to the attacker's computer.

To increase performance, a web-server typically caches translations from human-readable domain name into a numerical IP address for a certain amount of time. If a server receives another request for the same resource it can reply without asking any other servers. DNS spoofing focuses on corrupting the cached answers, either through software exploits or protocol weaknesses. The attack is difficult to detect, and very difficult to guard against. The payoff can be huge enough if the attackers were successful.

Traditionally the DNSSEC is often deployed to mitigate the risks.

II. Related work

There are a large number of works related to the problem. Reference [1] is devoted to defense against DNS Man-In-The-Middle Spoofing. Paper [2] presents the network traffic redirecting toward a fake DNS server on a Local Area Network (LAN). In the [3] discussed the main approaches to DNS protection against spoofing and poisoning attacks. In the conference paper [4] there is a security analysis related to the cache poisoning attacks in the domain name systems.

Neural network based spoofing detection description one can find in [5]. Implementation and analysis of identity spoofing attack using epidemic routing protocol in DTN presented in [6]. According to [6], the most effective used method for preventing and detecting of spoofing attack is hop count filtering method by building IP2HC Table. Paper [7] presents various aspects of hop count filtering method and its modifications to prevent and mitigate attacks.

Paper [8] presents the configuration of IoT network on which the authors are planning to test the application of the proposed method to network of IoT devices. In the [9] the comparative evaluation of spoofing defenses is presented.

III. METHOD

Spoofing detection is performed using an artificial RNN over a whole OSI data link layer data frame. RNNs are designed to learn sequence data. We extract only headers from frames, packets, segments, and high level protocols data structures and use those as features. These data continuously pass through the input layers of RNN within the time window in binary format. The architecture of RNN is Multiple Input One Output. The output of the last neural layer represents the output at the end of the each data frame. The training dataset training set consists of 100000 frames, the validation/development set contains 10000 frames, and the test set contains 10000 frames. The data were collected in experiment with network setup. We used the TensorFlow and Keras frameworks in our work. The Tensorboard was used for visualization of training scalars and neural network structures. Training of the model was performed using conventional server with Tesla T4 GPU with 16280 MiB of video memory (NVIDIA-SMI 450.51.05, Driver Version: 418.67, CUDA Version: 10.1). We used post-predict evaluation in order to evaluate the model. Test set went through the prediction method. After that, predictions were compared to the ground truth and the confusion matrix was derived. The following class-wise macro/micro-averaged and weighted metrics were obtained from the confusion matrix: error rate, accuracy, true positive rate (TPR, recall), positive predictive value (PPV, precision), etc.

IV. RESULTS AND CONCLUSION

We present the results of the research in form of accuracy assessment. The result shows that applying RNN gives the accuracy of 0.74. The overall purpose of the study was to prove the feasibility of the efficient detection of spoofing attack using recurrent neural network. Our main finding suggests that the use of RNN results in the performance that should be improved. The limitation is that data collected with experimental setup might have different properties then real. Therefore, real data is preferable to use for training further models. In our future works, we will add more features and test the accuracy which will give us a clear picture of the importance of each feature and show steps for further research.

REFERENCES

[1] Bai X., Hu L., Song Z., Chen F., Zhao K. (2011) Defense against DNS Man-In-The-Middle Spoofing. In: Gong Z., Luo X., Chen J., Lei J., Wang F.L. (eds) Web Information Systems and Mining. WISM 2011. Lecture Notes in Computer Science, vol 6987. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23971-7_39

[2] Maziar Janbeglou, Mazdak Zamani and Suhaimi Ibrahim, "Redirecting network traffic toward a fake DNS server on a LAN," *2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, 2010, pp. 429-433, doi: 10.1109/ICCSIT.2010.5565196.

[3] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal and A. Ibrahim, "DNS Protection against Spoofing and Poisoning Attacks," *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, Beijing, 2016, pp. 1308-1312, doi: 10.1109/ICISCE.2016.279.

[4] R. Bassil, R. Hobeica, W. Itani, C. Ghali, A. Kayssi and A. Chehab, "Security analysis and solution for thwarting cache poisoning attacks in the Domain Name System," *2012 19th International Conference on Telecommunications (ICT)*, Jounieh, 2012, pp. 1-6, doi: 10.1109/ICTEL.2012.6221233.

[5] Lumezanu C, Arora N, Chen H, Zong B, Daeki CH, Li M, inventors; NEC Laboratories America Inc, assignee. Neural network based spoofing detection. United States patent application US 16/101,794. 2019 Mar 28.

[6] Rani, S., Abhilasha, E., and Jindal, E. S., 2015. "Implementation and Analysis of Identity Spoofing Attack Using Epidemic Routing Protocol in DTN". International Journal of Current Engineering and Scientific Research (IJCESR). 2(12).

[7] H. Wang, C. Jin and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," in *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 40-53, Feb. 2007, doi: 10.1109/TNET.2006.890133.

[8] M. Kozlenko and M. Kuz, "Joint capturing of readouts of household power supply meters," *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, Lviv, 2016, pp. 755-757, doi: 10.1109/TCSET.2016.7452172.

[9] J. Mirkovic and E. Kissel, "Comparative Evaluation of Spoofing Defenses," in IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 218-232, March-April 2011, doi: 10.1109/TDSC.2009.44.