System for estimation CVSS severity metrics of vulnerability based on text mining technology

A.V. Nikonov[1], A.M. Vulfin[1], V.I. Vasilyev[1], A.D. Kirillova[1], V.A. Mikhailov[2]

[1]*Ufa State Aviation Technical University, K. Marks st. 12, Ufa, Russia, 4500772*
[2]*"Frodex OOO", Parkhomenko st. 133/1, Ufa, Russia, 450000*

Abstract

Paper presents a system for automated construction of the base vulnerability characteristics vector (CVSS vector) and the calculation of vulnerability severity assessment (CVSS base score) based on the analysis of the vulnerability description data using natural language processing (NLP) and text mining tools.

There were 100000 records taken from NVD vulnerability database as the initial dataset. Preprocessing of the original data consists of filtering irrelevant characters and words and lemmatization. The vector of formal features of textual descriptions is formed by the pretrained Google AutoML Natural Language model using paragraph2vec vector nesting evaluation. To assess the vulnerability vector for each component, a neural network regression model is used.

To assess the quality of constructing the CVSS vector and score using NLP methods, a comparison between NLP and the Bag-of-Words and TF-IDF feature generation technologies was performed.

As a result of the research, it was found that the traditional approach shows the accuracy of constructing the vulnerability vector within 80-85%, while the NLP-based approach showed the result of about 85-90%. At the same time, as a further development, it is advisable to consider the stage of reducing the dimension of the feature vector using the PCA and UMAP methods.

Keywords

Vulnerability, natural language processing, cybersecurity, machine learning, text mining

1. Introduction

In areas related to software audit and inventory, it is very important to have up-to-date information on existing vulnerabilities in order to effectively plan measures to improve the security of controlled objects. It is necessary to understand the importance of quickly determining the degree of danger, because from the moment of vulnerability disclosure, the likelihood of its exploitation by hackers increases many times over, since there is no information about the severity and characteristics of the vulnerability, which complicates the planning and implementation of protection measures.

Recent trends show that an increasing number of cyberattacks and software and hardware vulnerabilities are recorded every day, and their analysis and severity assessment takes an increasingly long time. In [1], it was shown that the assessment of the average analysis interval for new vulnerabilities takes 132 days after their registration.

The goal of the paper is to create a system for automated construction of the base vulnerability characteristics vector and the calculation of vulnerability severity assessment based on a textual description of the vulnerability, which will reduce the efficiency of exploiting new vulnerabilities.

Existing approaches [2, 3] are mainly aimed at predicting the likelihood of exploitation of a vulnerability, or at severity prediction only; other researches [4, 5, 6] describe the construction of a vulnerability vector, however, they use classical approaches of data processing. In this paper, the object of study is textual descriptions of vulnerabilities, and natural language processing tools are used to take into account contextual relationships in the textual description.

2. Model description

There were 100 000 records taken from NVD vulnerability database as the initial dataset. This database is maintained by the US National Institute of Standards and Technology (NIST) [7] – this organization analyzes vulnerabilities and assigns vectors and scores to them. The dataset structure contains the unique name of the vulnerability, textual description, score (if any), and vector (if any).

Further work is being done on the textual description. First, the description is preprocessed – punctuation marks, stop words and numbers are removed. Next, lemmatization is carried out – the words are transformed to their initial form, which reduces the number of actual duplicates.

Further processing consists of data labeling performed using pretrained Google AutoML Natural Language model using paragraph2vec vector nesting evaluation. To assess the vulnerability vector for each component, a neural network regression model is used.

To assess the quality of constructing the CVSS vector and score using NLP methods, a bunch of Bag-of-Words and TF-IDF algorithms is used as a comparative approach to feature extraction.

3. Results and conclusion

During the experiment, dataset was divided into training (60 000 records) and test samples (40 000 records). The classical approach based on BoW + TF-IDF showed the accuracy of constructing the vulnerability vector within 85%, while the approach based on NLP showed the result of about 90%. The severity score calculated on the basis of the constructed vector differs from the existing one by no more than 2%.

As a further development, it is advisable to consider the stage of reducing the dimension of the feature vector using the PCA, UMAP approaches to reduce the complexity of the applied regression models and prevent their overfitting.

4. Acknowledgments

The reported study was funded by RFBR, project number 20-08-00668 and 19-07-00972.

5. References

[1] Chen, H. VEST: A System for Vulnerability Exploit Scoring & Timing / H. Chen, J. Liu, R. Liu, N. Park, V. Subrahmanian // Proceedings of the 28 International Joint Conference on Artificial Intelligence. – Macao, China. – 2019. – P. 6503-6505.

[2] Leverett, É. Vulnerability Forecasting: In theory and practice / É. Leverett, M. Rhode, A. Wedgbury // ArXiv preprint: 2012.03814. – 2020. – P. 22.

[3] Feutrill, A. The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay / A. Feutrill, D. Ranathunga, Y. Yarom, M. Roughan // 6 International Symposium on Computing and Networking (CANDAR). – 2018. – P. 1-10.

[4] Elbaz, C. Fighting N-day vulnerabilities with automated CVSS vector prediction at disclosure / C. Elbaz, L. Rilling, C. Morin // Proceedings of the 15 International Conference on Availability, Reliability and Security. Ireland. – 2020. – P. 1-10.

[5] Jacobs, J. Exploit Prediction Scoring System (EPSS) / J. Jacobs, S. Romanosky, B. Edwards, M. Roytman, I. Adjerid // ArXiv preprint: 1908.04856. – 2019. – P. 22.

[6] Khazaei A. An automatic method for CVSS score prediction using vulnerabilities description / A. Khazaei, M. Ghasemzadeh, V. Derhami // Journal of Intelligent & Fuzzy Systems. – 2016. – Vol. 30(1). – P. 89-96.

[7] National Vulnerability Database Web Site [Electronic resource]. – Access mode: https:// https://nvd.nist.gov/vuln (10.01.2021).