RADemics

Ensemble Learning Frameworks for Improving the Accuracy of Zero-Day Exploit Detection

V.Samuthira
Chennai Institute of Technology

12. Ensemble Learning Frameworks for Improving the Accuracy of Zero-Day Exploit Detection

V.Samuthira Pandi , Department of ECE , Centre for Advanced Wireless Integrated Technology,Chennai Institute of Technology, Chennai. samuthirapandiv@citchennai.net.

Abstract

The detection of zero-day exploits presents a significant challenge in modern cybersecurity, as these attacks exploit unknown vulnerabilities before they are recognized and patched. Ensemble learning models have emerged as a promising approach to address this challenge by combining multiple base learners to enhance prediction accuracy and robustness. The performance of these models heavily depends on the quality and relevance of the features used during training. This chapter explores advanced strategies for improving ensemble learning accuracy in the context of zero-day exploit detection through sophisticated feature engineering techniques. The integration of external data sources, such as Common Vulnerabilities and Exposures (CVEs) and Indicators of Compromise (IoCs), plays a crucial role in enriching the feature set and enabling the detection of previously unseen attack patterns. Additionally, the chapter delves into the importance of data preprocessing, including cleaning, scaling, and dimensionality reduction, to optimize the data for ensemble models. Sensitivity analysis is highlighted as a key method for evaluating feature contributions, allowing for a deeper understanding of the factors influencing attack detection. By emphasizing domain-specific feature engineering and the continuous refinement of detection systems, this chapter provides a comprehensive approach to enhancing the effectiveness of ensemble models for zero-day exploit detection. The insights presented are intended to guide future research and practical applications in securing systems against evolving cyber threats.

Keywords: Zero-Day Exploit Detection, Ensemble Learning, Feature Engineering, CVEs, IoCs, Sensitivity Analysis.

Introduction

The detection of zero-day exploits has become a central concern in the realm of cybersecurity [1]. These attacks target vulnerabilities that are unknown to security vendors or the affected system developers, leaving the systems exposed to malicious threats until the vulnerabilities are discovered and patched [2]. Zero-day exploits are particularly dangerous because they are often difficult to detect using traditional security measures, which rely heavily on known attack signatures [3]. As cyber threats continue to evolve, there is a growing need for more effective detection mechanisms capable of identifying these unseen vulnerabilities in real time [4]. Ensemble learning, a machine learning technique that combines the outputs of multiple base models, has emerged as a promising solution for improving the accuracy and robustness of zero-day exploit detection systems [5]. By aggregating diverse learning algorithms, ensemble models

can enhance the system's ability to detect novel attack patterns and mitigate the risks associated with zero-day vulnerabilities [6].

The success of ensemble learning models in detecting zero-day exploits largely depends on the quality of the features used for training the models [7]. Feature engineering is a crucial step in the machine learning pipeline that involves selecting, modifying, and constructing relevant input data to improve the performance of the model [8]. In the case of zero-day exploit detection, feature engineering can be a complex and multifaceted process, as it requires extracting meaningful information from large and heterogeneous data sources [9]. Features such as network traffic patterns, system call sequences, and software configurations can provide valuable insights into the presence of vulnerabilities [10]. Domain-specific knowledge, such as information from Common Vulnerabilities and Exposures (CVEs) and Indicators of Compromise (IoCs), can further enhance the feature set, enabling models to identify patterns related to known vulnerabilities and previous attacks [11].

External data sources, including CVEs and IoCs, play an important role in improving the feature sets for zero-day exploit detection [12]. CVEs provide a comprehensive database of publicly disclosed vulnerabilities, which can be leveraged to identify software or hardware weaknesses that may be targeted by cybercriminals [13]. By integrating CVEs into the feature engineering process, ensemble learning models can gain access to valuable contextual data about known vulnerabilities, allowing them to detect exploit attempts targeting those weaknesses [14]. Similarly, IoCs, which include specific evidence of past cyberattacks, such as IP addresses, file hashes, or malicious domain names, provide critical information that can be used to detect emerging threats [15]. When incorporated into ensemble models, these external data sources enhance the model's ability to identify similarities between ongoing system behavior and previous attack patterns, thereby increasing the chances of detecting zero-day exploits [16].

Data preprocessing is another critical aspect of optimizing ensemble learning models for zero-day exploit detection [17]. Raw data collected from various system logs, network traffic, and sensor readings often contains noise, missing values, and inconsistencies that can hinder the performance of machine learning algorithms [18]. Data preprocessing techniques, such as normalization, scaling, and imputation, are essential for cleaning and transforming this data into a format suitable for model training [19]. These techniques help improve the convergence speed and overall accuracy of the ensemble models. Additionally, dimensionality reduction methods, such as Principal Component Analysis (PCA) or t-SNE, can be used to reduce the complexity of the feature space by eliminating irrelevant or redundant features [20]. By carefully preprocessing data before feeding it into ensemble models, the risk of overfitting is minimized, and the detection accuracy is improved [21].

Sensitivity analysis is an important tool for understanding the contribution of individual features to the overall performance of ensemble models in zero-day exploit detection [22]. Sensitivity analysis helps evaluate how changes in the values of specific features affect the model's predictions, providing insight into which features are most important for detecting zero-day attacks [23]. Techniques such as feature importance ranking and perturbation analysis can be employed to identify critical features that significantly impact the model's performance [24]. This analysis enables the identification of key features that should be prioritized for model optimization. It also helps uncover any interactions between features that may contribute to improved detection accuracy. By understanding the contributions of each feature, researchers can refine their feature

sets, optimize model training, and ensure that the ensemble model remains agile in the face of evolving threats [25].