Assignment#1

Hussien Tarek Ismail Abdelrazik
300389897

Selected Paper

- Title
  Encrypt DNS Traffic: Automated Feature Learning Method for Detecting DNS Tunnels
- Authors
  Shuai Ding, Daoqing Zhang, Jingguo Ge, Xiaowei Yuan & Xinhui Du

Summary

the paper tries to accurately detect hidden DNS Tunnels that are encrypted by DoH which makes the task more challenging & harder for detecting data exfiltration as it prevents packet inspection & domain name detection & ML analysis would require manual feature extraction which prevents online detection. this is solved by extracting raw flow sequence from encrypted traffic & embedding it to vector space then feeding it to the bidirectional Gated Recurrent Unit (Bi-GRU) based variational autoencoder (VAE) with attention mechanism following the encoder part. The study utilized a publicly available dataset containing three categories of DNS tunnel traffic: Iodine, Dns2tcp, and Dnscat2. To evaluate its performance, the proposed model was compared against 6 other models including Naive Bayes, Random Forest, Support Vector Machine, FS-Net, LSTM-AE & LSTM-VAE. The results demonstrated that the proposed model achieved superior accuracy, precision, recall, and F1-score for nearly all types of DNS tunnels & even for the models that had close accuracy to the proposed model they didn't perform as efficiently as the proposed model did or even with fewer parameters. Moreover, the inclusion of an attention mechanism in the proposed model showcased its effectiveness for capturing traffic flow contextual information. Additionally, experiments were conducted to assess the detection capability of unknown abnormal traffic which indicated that the proposed model displayed strong proficiency in detecting such anomalies. The primary conclusion of the study is that an end-to-end deep learning technique, utilizing a variational autoencoder neural network, is successful in identifying encrypted DNS tunnel traffic. This approach outperforms traditional machine learning models and baseline deep learning models in terms of detection accuracy. Unlike traditional methods, it doesn't rely on analyzing the content within DNS packets and instead automatically captures flow sequences, eliminating the need for complex feature engineering. The inclusion of an attention mechanism helps in setting thresholds and consolidating abnormal data. It's worth noting that the length of sequences also affects detection performance. Overall, this proposed model is highly effective in detecting previously unknown instances of abnormal traffic.

Critical Review

- Research Goal

The paper's primary objective is to surpass the capabilities of conventional machine learning models in detecting encrypted DNS tunnels by using deep learning. The attention mechanism's impact and the flow sequence length's effect on detection performance are also explored.

- Clarity

While well-structured, the paper assumes readers have a background in machine learning, which may require some readers to spend extra time grasping technical details. A minor symbol notation error is noted, and the absence of a dedicated discussion and future work sections but their content is mentioned in other sections.

- Related Works

The paper provides a comprehensive review of related research, offering essential context for the proposed method. It focuses on popular machine-learning methods but should caution against less popular but potentially superior solutions & could have concentrated solely on the literature about encrypted traffic.

- Methods

The paper introduces a Bi-GRU based VAE model with an attention mechanism for detecting DNS tunnels and encrypted traffic through semi-supervised learning. It compares its approach to traditional machine learning and basic deep learning & AE models, ensuring a clear and informative presentation.

- Results and Claims

The paper claims superiority in detection performance, achieving an F1-Score of nearly 99% with its proposed model. It emphasizes the model's ability to detect unknown forms of encrypted DNS tunnel traffic through semi-supervised detecting unknown previously unknown types of encrypted DNS tunnel & argue that the attention mechanism effectively concentrates the distribution of abnormal data & aiding thresholding process.

- Support of Results and Claims

The claims are substantiated through cited references and a comprehensive series of experiments. These experiments are conducted fairly, employing the same dataset and evaluation metrics across all methods. The paper showcases the practical utility of the proposed model through real-world implementation. However, their assertion that only PL, PD, and IAT are the sole valuable features lacks strong evidence or substantiation.

- Missing Claims and Results

Exploring the method's limitations, sensitivity to different DNS tunneling techniques, performance in diverse network configurations, and validation on a larger dataset, the incorporation of advanced evaluation metrics is also suggested & investigating the potential connection between performance decline at a sequence size of 128 and the use of 128-sized input embedding vectors and hidden layers.

- Discussion

While lacking a dedicated discussion section, the paper effectively addresses critical points within the "Result & Analysis" subsection of the evaluation section. It considers the merits and drawbacks of the proposed method, its versatility, and future research possibilities. However, a deeper exploration of limitations is recommended.

- Future Work

The authors could enhance their method by exploring different neural network architectures, transfer learning, domain adaptation techniques, and the impact of various encryption protocols. Addressing client obfuscation techniques and alternative approaches for handling insufficient flow length are also advised rather than padding.