Context-aware pre-trained models for intrusion detection systems

Mohamed Hashim Changrampadi
Doctoral Student
Chalmers University of Technology, Sweden
hashimm@chalmers.se

Abstract:

An Intrusion Detection System (IDS) is a crucial part of the cybersecurity infrastructure to monitor network traffic and provide alerts on any suspicious or malicious traffic in real-time or near real-time. These early alerts can prevent potential threats or mitigate the impact of detected attacks. As cyber threats continue to evolve in complexity, the need for IDS solutions that can dynamically adapt and effectively mitigate unseen attacks has paved way to Machine Learning based IDS.

Recent advancements in computational hardware have significantly enhanced the performance of machine learning-based IDS, potentially making them a better alternative to traditional rule-based approaches in several application scenarios. Major advantages of ML-based IDS are the ability to adapt and learn emerging threats, handle large and complex network traffic, continuously learn from new data, and improve detection accuracy. However, training a robust ML-based IDS often relies on massive training data with labeled attack samples. Several IDS datasets are available which are built on test-bed environments that emulate normal and malicious traffic; however, extracted features presented in the dataset make the AI model prone to bias. Moreover, these AI models need high computational resources to be trained and may not be suitable to be deployed in a resource-constrained environment.

These limitations can be addressed by training a foundation model to learn raw network traffic and then fine-tuning the model for specific attacks or an infrastructure. We investigate context-aware IDS that are trained on raw traffic data to learn subtle patterns of malicious traffic with high granularity. Preliminary results show that the fine-tuned models perform equally or better than the ML-based IDS model trained from scratch and consume less computational resources on deployment.