Machine Learning-based Intrusion Detection for Virtual Infrastructures

Mayank Arora, Integrated Masters in Computer Engineering

University of Dublin, Trinity College, 2022

Supervisor: Dr. Stefan Weber

There has been a shift from running applications in virtual machine-based environments to container-based environments in recent years. Although this shift has provided a better platform for deploying scalable applications, the tools to secure container-based environments from unknown attacks are still being developed.

This research has focused on enhancing security for applications deployed in Kubernetes. In particular, a Network-based Intrusion Detection System (NIDS) was proposed that uses an autoencoder, an unsupervised artificial neural network, to flag potentially anomalous packets. The autoencoder was trained on packets flowing through a Kubernetes node running an application, which created a baseline for normal behaviour. For testing the IDS, various port scans and dictionary attacks were launched against the application deployed in the virtual infrastructure. The IDS accurately detected the deviation from expected behaviour and categorised the packets as anomalous.

As part of the evaluation, we also compared autoencoders against other unsupervised detection algorithms such as IsolationForest and DBSCAN, and a supervised learning approach. Preliminary results show that a combination of signature-based and machine learning approaches is necessary for a comprehensive detection of intrusions in Kubernetes cluster.