Chair of Network Architectures and Services
School of Computation, Information, and Technology
Technical University of Munich

Thesis B.Sc.

HiWi

Local AI-based Network Anomaly Detection

Motivation

In previous work, we developed a tool able to detect anomalies in network flows. Examples for anomalies are connections between hosts which are unexpected, or communication from/to ports that should not be active, etc.
The model ”describing” the expected behavior of our network was created using an autoencoder. It was trained with a data set that contains packet traces from a large industrial network spanning multiple production sites. An autoencoder is a special architecture of an artificial neural network. It learns to encode training data into a lower-dimensional representation and decodes it back to its original form. Once trained, this model can be used to reconstruct observed network flows. If a flow has a significantly higher reconstruction error than the others, we consider it to be an anomaly.
So far, we have tested this approach on a training data set that probably exceeded the ability of the autoencoder as the size of the observed network was too big. Despite this fact, our approach showed promising results.
In this thesis, we want to revise the previous work. Your task is to train models of smaller segments of the entire network capture that reflect, for instance, an individual production site. Our hypothesis is, that the autoencoder model performs better when the network is smaller. Your next task is to confirm or reject this hypothesis. For this step, an approach of injecting certain anomalies (e.g. ICMP sweeps, port scans, DoS attempts, etc.) into the network capture is needed. Using the anomaly detection tool, you should be able to identify the injected traffic. Using standard metrics, you can finally compute the performance of the tool.
This B.Sc. topic can be extended by a HiWi activity.

Tasks

- Recreate the previous work’s results to familiarize yourself with the topic
- Train models of smaller network segments
- Create (or adapt) a tool able to inject anomalies into the network capture
- Evaluate the performance of the new models using the anomaly injection tool

Requirements

- Skills in AI methods and tools
- Basic networking knowledge

Contact

Christian Lübben luebben@net.in.tum.de
Holger Kinkelin kinkelin@net.in.tum.de
Lars Wüstrich wuestrich@net.in.tum.de