Prof. Dr.-Ing. habil. Falko Dressler
Data Communications and Networking – TKN

Technische Universität Berlin

Master's Thesis

Adoptive Anomaly Detection: Batch Learning

A firewall is well-known as the first layer of defense for your network. However, intruders developed new techniques to bypass the firewall and gain access to the network. Following, Intrusion Detection System (IDS) is introduced as a new layer of defense after the firewall to make the intruders' life more painful than ever.

The current volume of network traffic is on a scale that an IDS which is developed based on the most accurate approach (Deep Packet Inspection) can not analyze it completely. Consequently, a significant amount of traffic can pass IDS without any investigation. To tackle the issue, one approach is to drop the normal traffic from further investigation and preserve the limited processing resources for analyzing suspicious traffic.

However, the high dynamic nature of the network traffic makes it challenging to implement such an approach. The normal behavior in the network is variable and consequently, it is essential to update the anomaly detection model accordingly.

Goals of the Thesis

You, as a well-prepared researcher, are in charge of developing an online learning Anomaly detection system with the help of Snort which is the most accurate Intrusion Detection System. During your journey toward your final thesis, you will be involved in many tasks such as:

- preprocessing data and extracting the most relevant part of them to train a ML algorithm.
- Train a ML algorithm to detect anomaly activity and evaluate its accuracy.
- Compare the result of your ML algorithm with Snort.
- Connect your ML algorithm to Snort via a data stream to improve the precision.
- Retrain your ML algorithm with Snort output in a predefined time interval to maintain the overall accuracy of the system.

Of course, you will not be alone in your journey and your supervisor will guide you to take each step and will provide you the necessary ingredients for your research. In the end, you will finish your journey by defencing your thesis and introduce yourself to the academic community with (a) valuable publication(s). Besides, you will have a repository to maintain that host a precious tool to protect the online activity of thousands of people

Keywords

Online Machine Learning, IDS, Snort, Network Security

Contact:
Hossein Doroud: <h.doroud@tu-berlin.de>

Website:
www.tkn.tu-berlin.de