Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

Network Monitoring and Attack Detection

Master thesis proposal

Analyzing and understanding network activity can be extremely challenging in large and heterogeneous networks. In case of security incidents, response teams often invest an significant part of their resources to understand the compromised network architecture and to identify suspicious activity pattern for subsequent investigations. These tasks can be improved in order to allow response teams to focus on the incident resolution instead of consuming resources on legitimate activity analysis.

In this thesis, a large set of raw network data (> 100Gb PCAP) will be provided to the student. The dataset includes benign network activities and dozens of real attacks performed by a red team during a large international cyber defense exercise. The goal of the thesis is to develop a method to make analyst's work more effective by including features such as network objects tagging, visualizing network activity tracking and identifying abnormal (malicious) activity patterns. The results of this thesis are expected to be used in a follow-up international cyber defense exercise in order to help the defense teams in identifying attacks as quickly as possible.

Contacts

This thesis is offered in collaboration with armasuisse Science and Technology and can be performed either at ETH or at the research labs of armasuisse in Thun. If you are interested in the topic, please contact:

- Roland Meier (meierrol@ethz.ch) or
- Dr. Luca Gambazzi (luca.gambazzi@armasuisse.ch)