Intrusion Detection using Streaming Network Telemetry

In [2] an approach was proposed to query a network to monitor current traffic and flows. It relies on special programmable hardware. An open question is if comparable functionality and performance can be achieved using general purpose PC hardware. Thus in this project we want to find out if a software-based streaming network telemetry system can be used to detect common attack patterns. A promising suitable architecture involves FlowScope [1] and a real-time database.

- Can complex attack patterns be efficiently detected in software?
- What are constraints and limitations?
- Implement user-modules for FlowScope, an interface to a real-time database and suitable queries
- Evaluate your solution with relevant network traffic traces w.r.t functionality and performance
- Motivation and autonomy


Kilian Holzinger holzinger@net.in.tum.de