Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc.

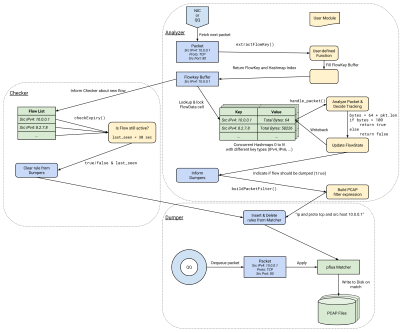
Thesis M.Sc.

IDP, Guided Research

Intrusion Detection using Streaming Network Telemetry

Introduction

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.



Research Questions

- Can complex attack patterns be efficiently detected in software?
- What are constraints and limitations?

Tasks

- 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

Requirements

- Motivation and autonomy

Literature

[1] P. Emmerich, M. Pudelko, Q. Scheitle, and G. Carle. Efficient Dynamic Flow Tracking for Packet Analyzers. In *CloudNet*, Tokyo, Japan, October 2018.

[2] A. Gupta, R. Harrison, M. Canini, N. Feamster, J. Rexford, and W. Willinger. Sonata: Query-driven streaming network telemetry. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '18, page 357–371, New York, NY, USA, 2018. Association for Computing Machinery.

Contact

Kilian Holzinger holzinger@net.in.tum.de