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

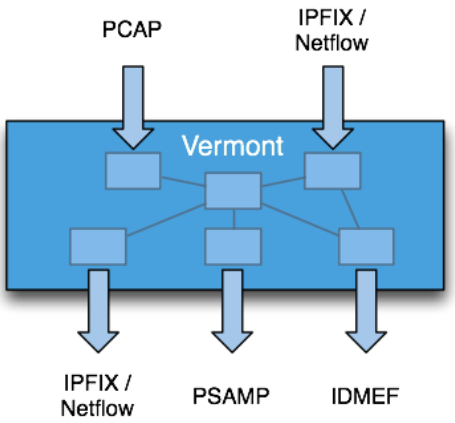
Thesis M.Sc.

IDP

Advanced Flow Functions for Traffic Anomaly Detection

Motivation

Flow data are an important source for various tasks such as network monitoring, accounting, attack detection and mitigation. NetFlow, IPFIX and sFlow are protocols which are used to provide flow information. We developed a software toolkit for the creation and processing of network flow data called Vermont (Versatile Monitoring Toolkit). Vermont was successfully used to handle flow data from our own Autonomous System as well as networks which provide more flow data.



You will add advanced flow features using special IPFIX Information Elements and data structures to Vermont. These advanced flow features could be distributions for packet sizes, TCP flags, TTL value, and timing information which go beyond the traditional IPFIX 5-tuple statistics. You will then evaluate the usefulness of these advanced flow features to detect traffic anomaly such as routing problems or unusual TCP connection states. Finally you will implement a dynamic reloading of the configuration using a RESTCONF interface to allow for on-demand reconfiguration by a controller.

Your Task

- Develop advanced flow features for Vermont
- Evaluate new features for traffic anomaly detection purposes
- Develop dynamic config reloading interface

Your Skills

- Extensive C++ knowledge (you should know how to properly use templates)
- Willingness to deep-dive into IPFIX, RESTCONF, YANG,...
- Painless usage of git SCM
- Previous experience of working on an Open Source project is a plus
- You live the GIYF motto

Contact

Oliver Gasser gasser@net.in.tum.de
Johannes Naab naab@net.in.tum.de

http://go.tum.de/306574