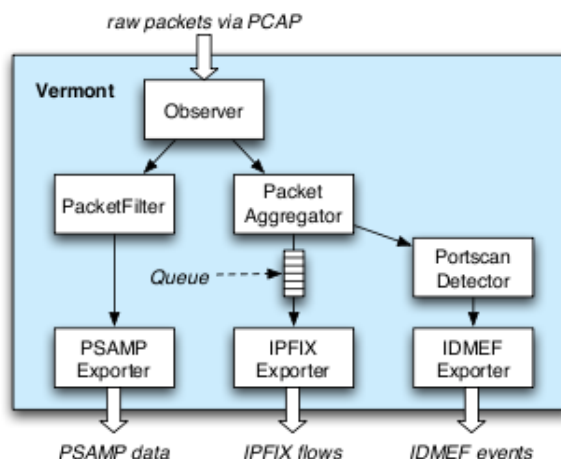


## Bachelorarbeit

# Beschleunigung der PCAP-Datenaufzeichnung für 10 GBit/s-Netze

### Beschreibung:

Mit der Anzahl der Internetnutzer und der angebotenen Dienstleistungen steigen auch Anzahl, Rate und Qualität von Angriffen. Viren und Würmer erreichen besorgniserregende Ausmaße. Im Rahmen eines Forschungsprojekts wurde unter anderem ein effizientes und verteiltes Netzwerkmonitoringsystem für Multi-Gigabit Netze implementiert. In diesem Zusammenhang wurde das Programm Vermont als Monitoringapplikation entwickelt, welche Daten in Datenströme, sogenannte Netflows, aggregiert und diese dann im IPFIX Format an weitere Module für anschließende Auswertung weiterleitet. Möglichkeiten der Auswertung werden beispielsweise durch Detektionsalgorithmen für die Portscanerkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.



### Aufgabenstellung:

Im Rahmen der Arbeit soll die Datenaufzeichnung über die PCAP-Schnittstelle für den Einsatz in 10 GBit/s Netzen optimiert und beschleunigt werden. PCAP (Packet Capturing) ist eine standardisierte Schnittstelle zum Aufzeichnen von IP Paketen, welche u.a. auch von tcpdump oder wireshark genutzt wird. Für den Einsatz in 10 GBit/s Netzen stellen jedoch die hohe Paketrage und die damit verbundene Interruptrate eine kritische Limitierung dar. Modernere Netzwerkkarten (z.B. die Serverkarte von Intel) erlauben eine Vorverarbeitung direkt auf der Hardware. Weiterhin sind optimierte PCAP Lösungen bekannt, welche durch Memory-Mapping und geeignete Ringpufferlösungen einen schnelleren Datenzugriff erlauben. Ziel der Arbeit ist es, diese Möglichkeiten genau zu erkunden und für Vermont zur Verfügung zu stellen. Dabei sollen u.a. beschleunigte Samplingalgorithmen implementiert werden. Abschliessend soll eine umfangreiche Experimentserie zur Bewertung der erreichten Beschleunigung durchgeführt werden.

### Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Statistik sind wünschenswert

### Ansprechpartner:

Falko Dressler <falko.dressler@uibk.ac.at>