

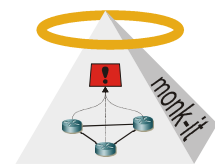
## Diplomarbeit

### Evaluation und Implementierung von Überlastschutzmethoden für einen Flowmonitor

#### Die dunkle Seite der Netzwerksicherheit – interessiert?

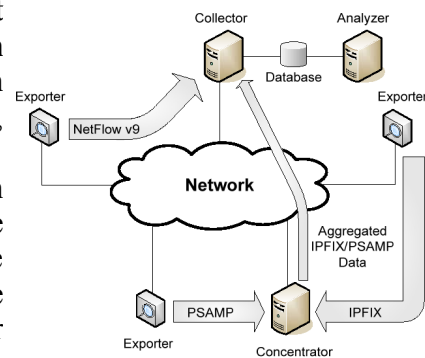
##### Beschreibung:

Mit der Anzahl der Internetnutzer und der angebotenen Dienstleistungen steigen auch Anzahl, Rate und Qualität von Angriffen. Viren und Würmer erreichen besorgniserregende Ausmaße. Es wird vom BSI ein Forschungsprojekt namens monk-it finanziert, welches unter anderem ein effizientes und verteiltes Netzwerküberwachungssystem fuer Multi-Gigabit Netze implementiert. Das Ziel ist es, eine intelligente, selbstorganisierende Monitoringumgebung zu schaffen, die Analysen (z.B. Angriffserkennung) vereinfacht.



In diesem Zusammenhang wurde das Programm Vermont als Monitoringapplikation entwickelt, welche Daten in Datenströme, sogenannte Netflows, einteilt und diese dann im IPFIX Format an weitere Auswertungsstationen, sogenannte Collectors, weiterleitet.

Die von Vermont überwachten Datenpakete werden anhand der Informationen im Paketheader in Datenströme zusammengefasst. Dies wird mit Hilfe einer Hashtabelle effizient durchgeführt. Um aus Angriffen entstehende Überlastsituationen kontrollieren zu können, wurden in der Forschung bereits Alternativen zu einer einfachen Hashtabelle vorgeschlagen.



##### Aufgabenstellung:

Es sollen in der Diplomarbeit mögliche Angriffsmethoden entworfen werden, indem beispielsweise speziell modifizierte Pakete zum Monitor geschickt werden und dadurch dessen Funktionsweise eingeschränkt wird. Ist dies erreicht, sollen für die Angriffe Gegenmassnahmen gefunden und implementiert werden.

##### Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Kryptographie sind wünschenswert.

##### Stichworte:

Monitoring, Angriffserkennung, Hashfunktion, Netflow, DoS

##### Ansprechpartner:

Tobias Limmer  
[tobias.limmer@informatik.uni-erlangen.de](mailto:tobias.limmer@informatik.uni-erlangen.de)  
Raum 06.158

und Dr. Falko Dressler  
[dressler@informatik.uni-erlangen.de](mailto:dressler@informatik.uni-erlangen.de)  
Raum 06.157