

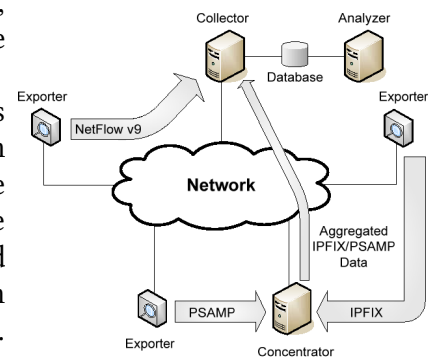
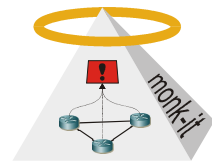
Studienarbeit

Entwicklung eines flowbasierten Detektors von Peer-to-Peer - Verkehr

Beschreibung:

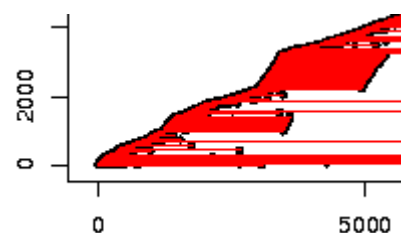
Mit der Anzahl der Internetnutzer und der angebotenen Dienstleistungen steigen auch Anzahl, Rate und Qualität von Angriffen. Viren und Würmer erreichen besorgniserregende Ausmaße. Es wird vom BSI ein Forschungsprojekt namens monk-it finanziert, welches unter anderem ein effizientes und verteiltes Netzwerküberwachungssystem 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, aggregiert und diese dann im IPFIX Format an weitere Module für anschließende Auswertung weiterleitet. Eine TCP/IP Verbindung wird dann anhand der IP-Headerdaten in zwei Datensätzen repräsentiert: Eine für den Hinweg, eine für den Rückweg. Möglichkeiten der Auswertung werden beispielsweise durch Detektionsalgorithmen für die Portscannererkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.



Aufgabenstellung:

In der Studienarbeit soll ein Auswertungsmodul für Netflowdaten implementiert werden. Ziel ist es, Rechner aufzuspüren welche Teil eines Peer-to-Peer Netzwerks bilden. Dazu werden in einem ersten Schritt mögliche Methoden zur Detektion ermittelt und evaluiert. Die vielversprechendste Methode wird daraufhin in Vermont als Modul implementiert und getestet.



Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Monitoring, Angriffserkennung, P2P, Flows

Ansprechpartner:

Tobias Limmer
tobias.limmer@informatik.uni-erlangen.de
Raum 06.158

und Dr. Falko Dressler
dressler@informatik.uni-erlangen.de
Raum 06.157