

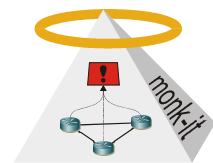


Studienarbeit

Evaluierung und Implementierung eines Detektors von Peer-to-Peer Netzwerkverkehr

Beschreibung:

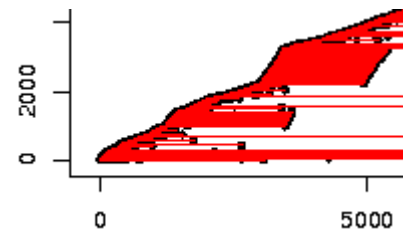
Mit der Anzahl der Internetnutzer und der angebotenen Dienstleistungen steigen auch Anzahl, Rate und Qualität von Angriffen. Viren und Würmer erreichen besorgniserregende Ausmaße. Es wird vom BSI ein Forschungsprojekt namens monk-it finanziert, welches unter anderem ein effizientes und verteiltes Netzwerküberwachungssystem 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:

Die Studienarbeit hat das Ziel einen Algorithmus weiterzuentwickeln, welcher zu Peer-to-Peer Netzwerken gehörende Rechner identifizieren kann. Ein herausragendes Merkmal der meisten Clients von Peer-to-Peer Netzwerken ist es, dass viele parallele Verbindungen zu anderen Peers aufgebaut werden. Dazu wurden in einer vorhergehenden Arbeit schon Erkennungskriterien definiert. Diese werden in einem ersten Schritt weiter evaluiert und mit Hilfe eines Vergleichs mit payloadbasierenden Analysemethoden auf ihre Effektivität überprüft. Anschließend wird der Detektionsalgorithmus als Modul im Monitoringsystem Vermont 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