

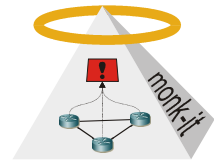


Diplomarbeit

Optimierung der Mehrprozessorunterstützung des Monitoring-Frameworks Vermont

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. Möglichkeiten der Auswertung werden beispielsweise durch Detektionsalgorithmen für Portscanerkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.



Aufgabenstellung:

Alle Funktionen des Monitoring-Frameworks Vermont werden intern in einzelne Module gekapselt, welche in beliebige Reihenfolge aneinandergeschaltet werden können. Um den aktuellen Trend zu mehreren CPU-Kernen innerhalb eines Rechners ausnutzen zu können, stellt Vermont Warteschlangen für die Datenübergabe zwischen in unterschiedlichen Threads ausgeführten Modulen bereit. Im Moment werden innerhalb dieser Warteschlangen für die Threadsynchrisation aufwändige, vom Betriebssystem zur Verfügung gestellte Mutexes für den Schutz kritischer Abschnitte verwendet. Dies zieht große Performanzeinbußen nach sich, insbesondere bei hoher Systemlast. Im Rahmen der Diplomarbeit sollen innerhalb des Frameworks für die Performanz wichtige kritische Abschnitte identifiziert und durch alternative Verfahren, wie sperrfreie Ringpuffer, ersetzt werden.

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Monitoring, Angriffserkennung, IPFIX, Flows, Vermont, sperrfreie Algorithmen, Multitasking

Ansprechpartner:

Tobias Limmer
limmer@informatik.uni-erlangen.de
Raum 06.133

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