

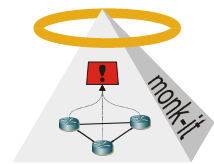


Diplomarbeit

Intelligente Datenselektion für Angriffserkennung in Netzwerken

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:

Im Rahmen des Projekts wird eine verteilte Analyseumgebung für Angriffserkennung implementiert, welche verschiedene Methoden für die Erkennung von Angriffen zur Verfügung stellt: Zum einen stehen leichtgewichtige Anomalieerkennungsalgorithmen basierend auf Netflowdaten zur Verfügung, zum anderen aufwändige Analysemethoden für Paketinhalte, welche nur geringe Datenraten verarbeiten können. Die aufwändigen Algorithmen sind meist nicht in der Lage, das gesamte Verkehrsaufkommen in Hochgeschwindigkeitsnetzen zu analysieren. Es muss also eine intelligente Datenselektion durchgeführt werden, um dennoch eine hohe Effizienz und Abdeckung in der Angriffserkennung zu erreichen. Im ersten Schritt soll dazu in dieser Diplomarbeit die Korrelation von Ereignissen aus geeigneten schnellen Anomalieerkennungsalgorithmen mit Ereignissen aus paketinhaltsbasierten Angriffserkennungssystemen wie Snort untersucht werden. Die Ergebnisse dieser Untersuchung werden dann im zweiten Schritt in der schon vorhandenen Analyseumgebung implementiert und evaluiert.

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Monitoring, Angriffserkennung, IPFIX, Flows, Vermont, Snort

Ansprechpartner:

Tobias Limmer

limmer@informatik.uni-erlangen.de

Raum 06.133

und Dr. Falko Dressler

dressler@informatik.uni-erlangen.de

Raum 06.157