

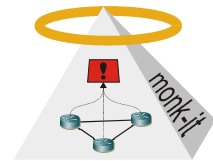


Studienarbeit

Signaturbasierte Angriffserkennung auf Flowdaten

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 Portscanerkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.

Aufgabenstellung:

Signaturbasierte Angriffserkennungssysteme besitzen eine Datenbank mit Signaturen, auf welche einkommende Netzwerkdaten geprüft werden. Wird eine Signatur in den Daten entdeckt, wird dies in Form eines sicherheitsrelevanten Ereignisses gemeldet. Dabei können die verwendeten Signaturen sich auf verschiedene Teile der Netzwerkdaten beziehen: Entweder auf Headerinformationen, oder auf Daten, welche sich innerhalb der Paketpayload befinden. Flowaggregation entfernt im Normalfall alle Payloaddaten und erhält nur Teile der Paketheaderdaten. Dieser Vorgang führt zu einer hohen Reduktion der Datenmenge. Dennoch ist es möglich, diese Daten mit verschiedenen Signaturdatenbanken abzugleichen und weiterhin Angriffe zu erkennen. Im Rahmen der Studienarbeit soll ein Modul im Monitoringframework Vermont für Signaturbasiertes Matching implementiert werden, welches Signaturen basierend auf Paketheaderinformationen effizient überprüft. Dazu wird ein Datenformat entwickelt, welches auf die Definition von flowbasierten Signaturen spezialisiert ist. Für dieses Format sollen zusätzlich Importmöglichkeiten geschaffen werden, um Signaturen automatisch aktualisieren zu können.

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