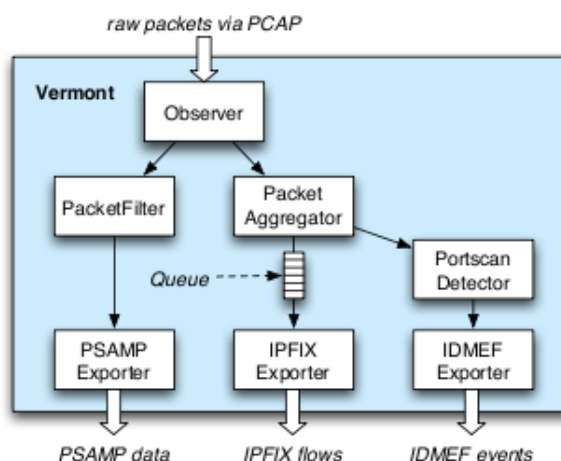


Masterarbeit

Anomalieerkennung zur adaptiven 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. Im Rahmen eines Forschungsprojekts wurde unter anderem ein effizientes und verteiltes Netzwerkmonitoringsystem für Multi-Gigabit Netze implementiert. 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 die Portscanerkennung, wie sie schon in dem Angriffserkennungssystem Snort eingesetzt werden, bereitgestellt.



Aufgabenstellung:

Im Rahmen der Arbeit soll eine verteilte Analyseumgebung für Angriffserkennung implementiert werden, 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 Masterarbeit 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 Statistik sind wünschenswert

Ansprechpartner:

Falko Dressler <falko.dressler@uibk.ac.at>