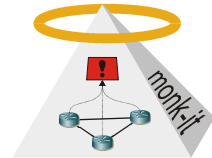


Diplomarbeit

Implementierung einer dynamischen Konfigurationsschnittstelle eines Netzwerküberwachungssystems

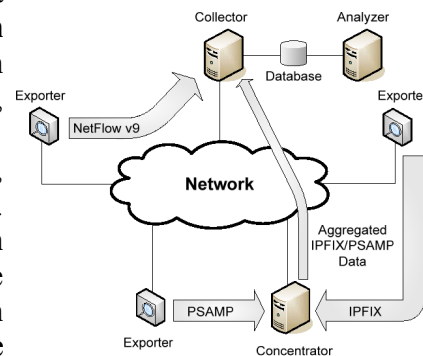
Beschreibung:

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 für Multi-Gigabit Netze implementiert. Das Ziel ist es, eine intelligente, selbstorganisierende Monitoringumgebung zu schaffen, die Analysen (z.B. Angriffserkennung) vereinfacht.



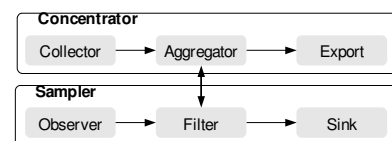
In diesem Zusammenhang wurde das Programm Vermont als Monitoringapplikation entwickelt, welche Daten in Datenströme, sogenannte Netflows, einteilt und diese dann im IPFIX Format an weitere Auswertungsstationen, sogenannte Collectors, über das Netzwerk weiterleitet.

Besonderer Wert wird dabei auf die Möglichkeit gelegt, auf bestimmte Ereignisse dynamisch reagieren zu können. Wird beispielsweise von einer Station erkannt, dass ein unbekannter Angriff durchgeführt wird, soll die überwachende Station die vom Angreifer geschickten Pakete detailliert auswerten. Dies ist nur möglich, wenn die Monitoringapplikation während der Laufzeit neu konfiguriert werden kann.



Aufgabenstellung:

Vermont soll um eine Schnittstelle erweitert werden, welche dynamische Rekonfiguration über das Netzwerk während der Laufzeit ermöglicht. Es soll dabei darauf geachtet werden, dass die Rekonfiguration in möglichst kurzer Zeit abgeschlossen wird, sodass wenige Pakete aus dem überwachten Netz verlorengehen. Dies erfordert strategisches Vorgehen bei der Umstrukturierung der modularisierten Struktur von Vermont.



Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, sind wünschenswert.

Stichworte:

Monitoring, Angriffserkennung, Rekonfiguration

Ansprechpartner:

Tobias Limmer und Dr. Falko Dressler

tobias.limmer@informatik.uni-erlangen.de

dressler@informatik.uni-erlangen.de