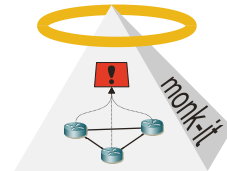


Diplomarbeit

Entwicklung eines verteilten IDS mit dynamischer Rekonfiguration der Netzwerksensorik

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 gefördert, welches unter anderem ein effizientes und verteiltes Netzwerküberwachungssystem für Multigigabit Netze implementiert. Das Ziel ist es, eine intelligente, selbstorganisierende Monitoringumgebung zu schaffen, die Analysen (z.B. Angriffserkennung) vereinfacht.

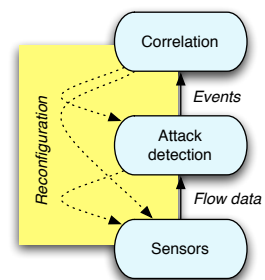


Aufgrund hoher Geschwindigkeiten in aktuellen Netzwerken ist es nicht möglich, den gesamten Inhalt aller übertragenen Pakete genau zu inspizieren und auf schadhafte Inhalte zu überprüfen. Deswegen ist es nötig, vorhandene Informationen möglichst früh zu komprimieren um die Datenmenge zu reduzieren. Diese Daten werden dann auf Anomalien überprüft. Erkannte Anomalien werden genauer analysiert, indem Teile des Netzwerkverkehrs durch einen payloadbasierenden Analysator (wie z.B. dem IDS Snort) überprüft werden und basierend auf diesen Auswertungen sicherheitsrelevante Ereignisse erkannt werden.

Aufgabenstellung:

Basis der Diplomarbeit ist das am Lehrstuhl entwickelte Ereigniskorrelationsframework Prism++, der Netzwerksensor Vermont, welcher Netzwerkanomalien erkennen kann, und dem öffentlich verfügbaren IDS Snort. Aus diesen Komponenten soll ein Modell eines verteilten Angriffserkennungssystems entwickelt werden, welches dynamisch auf aktuelle Auslastung und erkannte Anomalien reagieren kann und vorhandene Ressourcen optimal auslastet.

Dieses Modell soll anschließend in einer Testumgebung realisiert und die Effektivität anhand von realem Netzwerkverkehr ausgewertet werden.



Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Netzwerksicherheit sind wünschenswert

Stichworte:

Monitoring, Angriffserkennung, Netflows, IPFIX, dynamische Rekonfiguration, IDS

Ansprechpartner:

Tobias Limmer
tobias.limmer@informatik.uni-erlangen.de
Raum 06.150

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