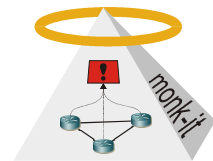


Diplomarbeit

Untersuchung von Angriffsmodellen und geeigneten Schutzmaßnahmen für Flowmonitore

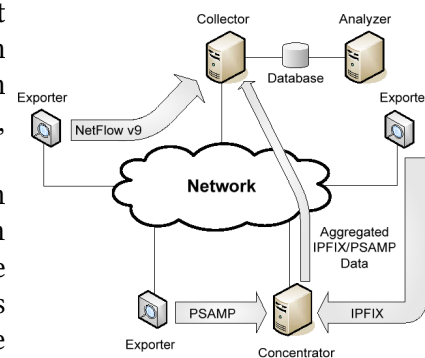
Beschreibung:

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, einteilt und diese dann im IPFIX Format an weitere Auswertungsstationen, sogenannte Collectors, weiterleitet.

Die von Vermont überwachten Netzwerkpakete werden anhand der Informationen im Paketheader in Datenströmen zusammengefasst. Durch die direkte, zustandsbasierte Analyse von Netzwerkdaten innerhalb von Vermont ist es für Angreifer möglich, gezielt dessen Funktionsweise auszunutzen: Es können spezielle Verkehrsmuster künstlich erzeugt werden, sodass die Funktionalität des Flowmonitors eingeschränkt wird und die Analyse der Netzwerkdaten nicht mehr lückenlos durchgeführt werden kann.



Aufgabenstellung:

Es sollen in der Diplomarbeit in einem ersten Schritt mögliche Angriffsmodelle auf Vermont entwickelt und deren Auswirkung analysiert werden. Daraus sollen mehrere Modelle ausgewählt werden und gezielt dafür Gegenmaßnahmen innerhalb von Vermont implementiert werden, sodass diese Angriffe nicht mehr oder nur stark erschwert durchführbar sind. Die Analyse und Evaluation soll theoretisch durchgeführt und mit experimentell ermittelten Ergebnissen bestätigt werden.

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Kryptographie sind wünschenswert.

Stichworte:

Monitoring, Angriffserkennung, Netflow, Denial-of-Service

Ansprechpartner:

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

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