Netzbasierte Angriffs- und Anomalieerkennung mit TOPAS

Lothar Braun und Gerhard Münz

Rechnernetze und Internet, Wilhelm-Schickard-Institut für Informatik, Universität Tübingen
{braunl|muenz}@informatik.uni-tuebingen.de

Die Erkennung von Denial-of-Service(DoS)-Angriffen und Würmern in großen Netzwerken mit hohen Bandbreiten stellt eine besondere Herausforderung dar. Der Einsatz konventioneller Intrusion-Detection-Systeme, wie z.B. Snort [MR99], ist dort problematisch, weil diese Netzwerkverkehr nur punktuell und nur bis zu einer gewissen Paketrate beobachten und untersuchen können. Das hier vorgestellte System *TOPAS* (Traffic flOw and Packet Analysis System) verarbeitet Verkehrsdaten, die von Netzwerkmonitoren über die Standardprotokolle Cisco Netflow [BC04] und IPFIX/PSAMP [BC06a, BC06b] exportiert werden. Die Netzwerkmonitore übernehmen dabei die Selektierung und Vorverarbeitung der Verkehrsdaten durch Paketfilterung, Sampling und Flow Accounting. Da Netzwerkmonitore auch für andere Aufgaben eingesetzt werden, z.B. zur Abrechnung des geflossenen Datenvolumens, lässt sich das System leicht in bestehende Netze integrieren.

TOPAS ist in der Lage, sowohl Flow-Daten, als auch Paketdaten zu verarbeiten. Dabei beschreiben die Flow-Daten Verkehrsströme, die in letzter Zeit an einem Netzwerkmonitor beobachtet wurden. Sie können verwendet werden, um Angriffe zu entdecken, die Änderungen in der Zusammensetzung der Flows verursachen. Paketdaten dienen dagegen zur Untersuchung einzelner Pakete und deren Inhalte, z.B. durch signaturbasierte Erkennungsverfahren.

Die Verkehrsdaten können von Monitoren stammen, die gleichzeitig verschiedene Stellen des Netzes überwachen. Dadurch können die Verkehrsdaten aus dem gesamten Netz mit einer einzigen Instanz des Systems auf Angriffe und Anomalien hin untersucht werden. In größeren Netzen und bei hohen Bandbreiten kann TOPAS aber auch verteilt betrieben werden, wenn das Verkehrsdatenvolumen die Verarbeitungskapazität einer Instanz übersteigt.

TOPAS besteht aus zwei Teilen: Einem Kollektor, der das System mit Netzwerkverkehrsdaten versorgt, sowie einem Modulsystem, das es erlaubt, in getrennten Modulen verschiedene Analysealgorithmen parallel auf die Verkehrsdaten anzuwenden. Die Module sind dabei auf die Erkennung bestimmter Angriffe oder Anomalien spezialisiert, z.B. auf die Erkennung von DoS-Angriffen, Port-Scans oder gefälschten Absenderadressen. Die Module können dynamisch gestartet werden, was eine ereignisgesteuerte Analyse der vorliegenden Verkehrsdaten ermöglicht. So kann beispielsweise ein permanent aktiviertes Modul eine wenig rechenintensive Erstanalyse der Daten vornehmen und, sobald ein Verdacht auf einen Anomalie vorliegt, eine genauere Analyse durch ein nachgestartetes Modul veranlassen, um die Anomalie zu klassifizieren, weiter gehende Analysen einzuleiten oder die Analyse abzubrechen, wenn sich die Anomalie als ungefährlich herausstellt.

TOPAS wird derzeit im Rahmen des EU-Projekts *Diadem Firewall* entwickelt und eingesetzt.

Literatur

[MR99] Martin Roesch: *Snort: Lightweight Intrusion Detection for Networks.* In *13th USENIX Conference on System Administration*, USENIX Association, 1999, Seiten 229–238.

[BC04] Benoit Claise: *Cisco Systems NetFlow Services Export Version 9.* RFC 3954, Okt. 2004.

[BC06a] Benoit Claise: *IPFIX Protocol Specification.* Internet-Draft, draft-ietf-ipfix-protocol-21, April 2006

[BC06b] Benoit Claise: *Packet Sampling (PSAMP) Protocol Specifications*, Internet-Draft, draft-ietf-psamp-protocol-05, März 2006