Transparentes Load-Balancing für Network Intrusion Detection Systeme

Matthias Vallentin* und Robin Sommer†

*TU München
vallentin{at}icsi.berkeley.edu

†ICSI
robin{at}icir.org

Network Intrusion Detection Systeme (NIDS) erkennen Verletzungen der Sicherheitsrichtlinien, indem sie den den Netzwerkverkehr auf bösartige Aktivitäten überwachen. Leistungsstarke Gbps-Netzwerke stellen jedoch neue Herausforderungen an ein NIDS. In Umgebungen mit hohem Datenaufkommen erreichen bisherige Ansätze, deren Architekturen auf Einzelbetrieb ausgelegt sind, häufig ihre Grenzen. Um der unzureichenden Rechenkapazität entgegen zu wirken, bieten Hersteller meist sehr teure, zugeschnitte Spezial-Hardware an. In unserer Arbeit stellen wir Methodiken zum *Clustering* und *Load-Balancing* von NIDS auf Standard-Hardware vor, die wir am Beispiel des Open-Source NIDS Bro [Pax99] in die Praxis umsetzen. Ferner integrieren wir einen Cluster in die Netzwerk-Infrastruktur des Lawrence Berkeley National Laboratory (LBNL, [LBL]), mit dem externe Verbindungen des Netzwerks und die DMZ überwacht werden.

Traditionelle Systeme verwenden zur Erkennung von Angriffen einen Satz Signaturen mit bereits existierenden Angriffen, die sie byteweise mit dem Datenstrom vergleichen. Bro verwaltet darüber hinaus einen genaues Abbild des Netzwerkzustandes, der policy-neutral erfasst wird. Das Konzept des *Independent State* [SoPa05] erlaubt es, diesen Zustand mehreren parallel laufenden Instanzen zugänglich zu machen und untereinander auszutauschen. Während bisherige Herangehensweisen nur aggregierte Informationen (z.B. Logs und Alarme) austauschen, kann Bro seine gesamten angesammelten Zustandsinformationen allen Instanzen bekannt machen. Diese Möglichkeit birgt ein großes Anwendungspotential im Hinblick auf eine verteilte Analyse mit höherer Transparenz [SoPa05].

Darauf aufbauend haben wir Bro um Mechanismen erweitert, mit denen ein skalierbarer NIDS-Cluster geschaffen werden kann. In Gbps-Netzwerken ist es damit möglich, sich nicht nur wie bisher aufgrund knapper Rechenkapazität auf eine Teilmenge des Netzwerkverkehrs zu beschränken, sondern die Analyse auf die vollständige Datenmenge auszuweiten. Insbesonders haben wird Bros Policy-Skripte für den Einsatz in einem Cluster protokollspezifisch angepasst. Die Erweiterungen erlauben eine feine Kontrolle der auszutauschenden Zustandsinformationen und bieten Unterstützung für unterschiedliche Cluster-Topologien.

Literatur

[LBL] Lawrence Berkeley National Laboratory. `http://www.lbl.gov`.

[Pax99] Vern Paxson. *Bro: A System for Detecting Network Intruders in Real-Time*. Computer Networks, 31(23-24):2435-2463, 1999.

[SoPa05] Robin Sommer und Vern Paxson. *Exploiting Independent State For Network Intrusion Detection*. In *Proceedings of the 21st Annual Computer Security Applications Conference*, 2005.