Zugriffskontrolle in komplexen verteilten Systemen: Paketfilternetze

Birger Tödtmann
Lehrstuhl Technik der Rechnernetze
Institut für experimentelle Mathematik
Universität Duisburg-Essen

Abstract. Der Einsatz von Mechanismen zur Kontrolle von Kommunikationsbeziehungen in IP-Netzwerken ist heutzutage mit den steigenden Risiken sowohl in Bezug auf die wirtschaftliche Nutzung als auch auf Sicherheit weitgehend alltäglich geworden. Insbesondere über den Gebrauch von Paketfiltersoftware, etwa mittels des Betriebs so genannter „Firewalls“ an Netzein- und -ausgängen, wird bereits auf Netzwerkebene eine technologisch ausgereifte Kontrolle über gewünschte und nicht-gewünschte Kommunikation in Organisationen ausgeübt.

Problematisch wird diese Praxis jedoch in komplexeren verteilten Szenarien, bei denen etwa Ein- und Ausgänge – also die Orte, an denen Paketfilter üblicherweise eingesetzt werden – nicht mehr klar definiert sind oder sich dynamisch verhalten, d.h. wandern. Umgebungen dieser Art nehmen zu: Netzbetreiber schließen sich zusammen (Netzgrenzen verschwinden), mobile Netzbereiche wandern über Betreiber hinweg, und die Verwaltung und Organisation von Netzen ist oft nicht mehr kongruent zur Topologie. Darüber hinaus werden Paketfilter inzwischen auch auf Endgeräten eingesetzt um eine nicht-authorisierte Kommunikation von Applikationen (Viren, Trojaner) zu verhindern. Da diese Endgeräte zunehmend mobil werden, ist hier oft auch eine Anpassung der Filterkonfiguration notwendig.

Im Rahmen der Entwicklung einer Sicherheitsarchitektur im Forschungsprojekt KING (Schlüssel-Komponenten für das Internet der nächsten Generation)[1] mit der Siemens AG wurde ein neues Zugriffskontrollverfahren auf Netzwerkebene entwickelt, das vor allem die bisher ungelösten Verwaltungsaufgaben bei der Konfiguration von Paketfiltern in den angesprochenen Problembereichen lösen soll.

Ausgehend von der Aufgabenstellung, in offenen IP-basierten Weitverkehrsnetzen Kontrollverbindungen von Steuerkomponenten besonders gegen Angriffe schützen zu müssen, können zunächst Schutzpfade definiert werden. Diese bestehen prinzipiell einfach aus Paketfilterkonfigurationen auf denjenigen Netzwerkknoten, über die eine zu schützende Kommunikationsbeziehung verläuft: alle Datenpakete, die vorgeblich zu dieser Verbindung gehören, aber nicht über den definierten Pfad eingehen, werden verworfen. Problematisch wird dieses Konzept allerdings mit Veränderungen, die eine automatisierte Wegesteuerung bei Pfadbrüchen einleitet. Die Paketfilterkonfigurationen würden dann nicht mehr zu dem neuen Pfad der zu schützenden Kommunikationsbeziehung passen und diese zum Einen nicht mehr schützen, zum Anderen mit hoher Wahrscheinlichkeit sogar behindern. Im KING-Projekt wurde daher ein Zugriffskontrollsystem entwickelt, das die möglichen Fehlerzustände im Netz und die zu erwartenden Reaktionen der Wegesteuerung vorausberechnet und dann gemäß einer definierten Risikotoleranz optimale Filterkonfigurationen ermittelt.

Die Herausforderung bei der Herstellung solcher Filternetze liegt in der Abschätzung wahrscheinlicher Wege, die eine zu schützende Kommunikationsverbindung selbst im Fehlerfall nehmen wird und dem Risiko eines Angriffs über bestimmte Netzwerkpfade. Bei einer Fehlkalkulation können zwei mögliche Zustände eintreten:

- „false positive“ – ein Verbotsfilter blockiert eine wichtige, umgeleitete Steuerverbindung
- „false negative“ – ein Erlaubnisfilter ermöglicht unbefugten Dritten, eine wichtige Steuerverbindung zu kompromittieren

Je nach Schadenshöhe für den einen oder anderen Fall können allerdings die jeweiligen Risiken (Schadenshöhe multipliziert mit der Wahrscheinlichkeit des Eintretens der Situation) kalkuliert und Paketfilternetze hergestellt werden, die dem Zugriffskontrollziel entsprechen. Im KING-Projekt wurde eine Implementierung in Java vorgenommen, die einen so genannten „Access Policy Configuration Point“ (APCP) realisiert. Der Anwender kann hier Schutzzieldefinitionen mit den Schadenshöhen angeben, die bei einer gegebenen Netzbeschreibung eine entsprechende Paktefilternetzkonfiguration generiert. Diese besteht aus den Paketfilterkonfigurationen aller betroffenen Netzelemente, den in diesem Konzept so genannten „Access Policy Enforcement Points“ (APEP). Der APCP kann diese zunächst generischen Filterkonfigurationen dann in die syntaktisch für die Netzknoten passenden Konfigurationsanweisungen konvertieren.

Im Vortrag werden das allgemeine Konzept, theoretische Überlegungen zu Paketfilternetzen sowie Implementierungsdetails vorgestellt, des Weiteren werden Effizienzuntersuchungen dargelegt.

[1] Gefördert durch die Siemens AG und dem Bundesministerium für Bildung und Forschung (Förder-Nr. 01AK045)