

Berichte aus der Telematik

Marcus Schöller

**Stabilität und Robustheit von
programmierbaren Vermittlungssystemen**

Shaker Verlag
Aachen 2006

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Karlsruhe, Univ., Diss., 2006

Copyright Shaker Verlag 2006

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN-10: 3-8322-5715-2

ISBN-13: 978-3-8322-5715-6

ISSN 0948-700X

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • E-Mail: info@shaker.de

Stabilität und Robustheit von programmierbaren Vermittlungssystemen

Dipl.-Inform. Marcus Schöller

Das ursprüngliche Design des Internets basierte auf einer strikten Aufgabenteilung zwischen Paketvermittlung im Netzinneren und den Anwendungen am Netzrand. Der Vorteil dieses Ansatz liegt in der Einfachheit der Funktionalität, die auf den Vermittlungssystemen benötigt wird. Um eine korrekte Weiterleitung der IP-Pakete zu gewährleisten, werden ausschließlich Informationen über alle bekannten Zieladressen und der dazugehörigen Wegeinformation benötigt.

Bricht man diese strikte Aufgabenteilung auf, indem man Dienste in das Netzinnere einbringt, so ermöglicht dies dem Netzbetreiber sowohl Dienste anzubieten, die Anwendungen seiner Kunden unterstützen, als auch Dienste einzusetzen, die den Betrieb des Netzes selbst erleichtern. Beispiele für solche Dienste können Datenformatsanpassungen und Datenformatsänderungen, wie auch Dienste zur Verkehrsaggregation, Angriffserkennung und viele mehr sein. Ein erster Schritt, der eine Aufweichung dieser Trennung darstellte, waren Proxy-Systeme, die für spezielle Anwendungen Dienste anbieten konnten. Solche Proxy-Systeme sind allerdings fest auf einige wenige Dienste spezialisiert. Der Forschungsbereich der aktiven und programmierbaren Netze hat das Ziel diese strikte Aufgabenteilung völlig aufzuheben, indem Vermittlungssysteme dynamisch und flexibel um Dienste erweitert werden können. Dazu werden die Vermittlungssysteme um eine offene Programmierschnittstelle erweitert, auf der diese neuen Dienste aufsetzen. Das Starten der Dienste wird entweder durch den Netzbetreiber selbst oder durch die Anwendungen des Kunden automatisch ausgelöst, indem entsprechende Signalisierungsnachrichten an die programmierbaren Vermittlungssysteme gesendet werden.

Neben dem Vorteil einer höheren Flexibilität muss aber auch das Risiko durch ein derart erweitertes Vermittlungssystem betrachtet werden. Für einen Angreifer stellt ein Vermittlungssystem ein äußerst attraktives Ziel für Denail-of-Service-Angriffe dar, da mit einem erfolgreichen Angriff meist nicht nur das System selbst, sondern auch weitere Systeme, die über das Vermittlungssystem erreicht werden, und deren Anwendungen betroffen sind. Im Wesentlichen konnten die folgenden allgemeinen Angriffspunkte identifiziert werden: Nutzung nicht autorisierter Dienste, Unberechtigte Dienstnutzung und Angriff auf die Signalisierung. Darüber hinaus gibt es ein Vielzahl von Angriffen, die auf der jeweiligen Funktionalität der Dienste beruhen, welche sich in zwei Klassen einteilen lassen: Ausnutzung eines Dienstes, um einen Denail-of-Service-Angriff gegen das programmierbare Vermittlungssystem selbst auszuführen und Verwendung eines Dienstes für Angriffe gegen andere Systeme. Die zweite Klasse dieser Angriffe lässt sich nicht systematisch durch einen generischen Ansatz des programmierbaren Vermittlungssystems verhindern und wurde deshalb im Rahmen dieser Arbeit nicht weiter betrachtet.

Bei der Untersuchung programmierbarer Vermittlungssysteme konnten drei Funktionalitäten identifiziert werden, die wesentlich zur Stabilität des Systems im Regelbetrieb und zur Robustheit gegen die genannten Angriffe beitragen: die Ressourcenverwaltung, die Dienstplatzierung und die dafür notwendige Signalisierung.

Da Dienste eines programmierbaren Vermittlungssystems sowohl in Software – Binärbibliotheken und Java-Bytecode – als auch in Hardware – DSPs und FPGAs – implementiert sein können, war es notwendig eine generische Ressourcenverwaltung zu entwerfen, die den Zugang zu Ressourcen und die Belegung der Ressourcen steuern kann. Dazu wurde eine zusätzliche Schicht zur Zugriffskontrolle der Systemschnittstelle hinzugefügt, die diese Aufgabe übernimmt und somit unabhängig von der Technologie ist, die zur Umsetzung des Dienstes verwendet wurde. Die Ressourcen-Konfiguration eines Dienstes legt fest, auf welche Ressourcen der Dienste zugreifen und wieviele er davon nutzen darf. Zusätzlich ist angegeben wieviel der jeweiligen Ressource mindestens von dem Dienst benötigt werden, um ausgeführt werden zu können. Zugriffe auf andere Ressourcen und eine Überbelegung der zugewiesenen Ressourcen wird von der Zugriffskontrolle verhindert.

Aufbauend auf dieser Zugangskontrolle unterstützt die Ressourcenverwaltung die Evaluation des Systems während des Aufsetzens eines neuen Dienstes, indem es Informationen über die vorhandene Hardware und den Grad der Belegung der Ressourcen bereitstellt. Soll auf einem programmierbaren Vermittlungssystem ein neuer Dienst gestartet werden, so muss überprüft werden, ob auf dem System genügend freie Ressourcen für die Ausführung dieses Dienstes vorhanden sind. Sollte das evaluierte System nicht genügend Ressourcen für den angeforderten Dienst bereitstellen können, so ist es bei einer Vielzahl von Diensten möglich, diese auf einem benachbarten Vermittlungssystem ausführen zu lassen, ohne dass dies Einfluss auf den Dienst selbst hat. Dazu mussten geeignete Strategien gefunden werden, die es erlauben programmierbare Vermittlungssysteme in der Umgebung des Systems zu evaluieren, das die Dienstanfrage entgegengenommen hat. Die Strategien unterscheiden sich je nach Art des Dienstes, wie z.B. Transparenz gegenüber dem Empfänger, dem Grad der Verteilung des Dienstes oder der Anzahl der Dienstkontexte. Daraus ergab sich die Folgerung, dass nicht eine Strategie für alle Dienste geeignet ist, sondern dass jeder Dienst eine eigens auf diesen angepasste Evaluationsstrategie mitbringen kann. So kann ein Dienst unter anderen auf Strategien wie eine Ring-, Pfad- oder Baum-basierte Suche nach weiteren programmierbaren Vermittlungssystemen zurückgreifen. Die Einsatzmöglichkeiten und Randbedingungen der unterschiedlichen Strategien bzgl. der Diensteseigenschaften wurde genau untersucht.

Für die Kommunikation mit dem programmierbaren Vermittlungssystem und der Systeme untereinander muss eine geeignete Signalisierung gefunden werden, die es erlaubt autorisierten Nutzern Dienste zu starten und ihre eigenen Dienste wieder beenden zu können. Dies bedeutet einerseits, dass eine Identifizierung des Nutzers während der Signalisierung unterstützt und andererseits, dass ein Mechanismus entwickelt werden muss, der verhindert, dass die Verarbeitung der Signalisierungsnachrichten zu einer Angriffsmöglichkeit auf das programmierbare Vermittlungssystem wird. Der Mechanismus der Signalisierungsumlenkung ermöglicht einen derartigen Schutz des programmierbaren Vermittlungssystems. Die Evaluation dieser Funktionalitäten zeigt deutlich, dass dieser Mechanismus das Vermittlungssystem vor Denial-of-Service-Angriffe mit hoher Datenrate schützen kann.

Die entwickelten Funktionalitäten wurde in den FlexiNet-Knoten – eine Umsetzung eines programmierbaren Vermittlungssystem auf Linux-Basis – integriert und im Rahmen verschiedener Prototypen evaluiert. Die erzielten Resultate erfüllen die in die Arbeit gesteckten Erwartungen und stellen eine solide Basis für den Aufbau eines stabilen und robusten programmierbaren Vermittlungssystems dar.