Mikrokerne als Universalbetriebssystem

Adam Lackorzynski, Hermann Härtig

TU Dresden, Betriebssystemegruppe

Die Betriebssystemegruppe von Prof. Hermann Härtig an der TU Dresden blickt auf eine gut 20-jährige Geschichte im Bereich Betriebssystemeforschung zurück. Seine Anfänge nahm die Entwicklung mit einer Kooperation mit Prof. Jochen Liedtke, der einen neuartigen und besonders schnellen Mikrokern in reinem Assembler entwickelt hatte. Er nannte den Mikrokern „L4“. Um die Geschwindigkeit von L4 zu bestätigen, wurde eine zu vorhandenen Systemen kompatible Applikation gesucht, und gefunden: L^{4}Linux. L^{4}Linux ist ein Linux-Kern, der an die Schnittstelle von L4 adaptiert wurde und als reines Applikationsprogramm läuft aber auch binärkompatibel zu bestehenden Linux-Programmen ist. Heutzutage würde man diese Technik als Virtualisierung bezeichnen. Benchmarks zeigten, dass die Applikationsleistung auf einem Mikrokern mit der einer herkömmlichen monolithischen Umgebung vergleichbar ist.

Bei der einfachen Ausführung von Linux-Programmen sollte es aber nicht bleiben. Die Kombination von Linux mit Echtzeitprogrammen auf einem System war dann ein nächster naheliegender Schritt. L^{4}Linux führt Linux-Programme aus, während Echtzeitprogramme direkt auf dem Mikrokern laufen, welcher sicherstellt, dass die Echtzeitprogramme immer Vorrang vor Linux-Programmen haben. Schnell stellte sich auch der Wunsch heraus, einen eigenen Mikrokern zu haben, der in einer Hochsprache entwickelt ist und die gewünschten Echtzeiteigenschaften erfüllt: Der „Fiasco“ Mikrokern entstand. Ein besonderes Merkmal eines Mikrokerns ist der kleine Funktionsumfang, was die Entwicklung von Programmen direkt auf dem Mikrokern mühsam macht. Um solche Entwicklungen zu erleichtern wurde das „L4Env – L4 Environment“ entwickelt, eine Entwicklungs- und Laufzeitumgebung für L4 Programme.

Nach einigen Jahren rückte das Thema Sicherheit immer mehr in den Fokus. Zur Konstruktion von sicheren Systemen bedarf es einer sicheren und soliden Grundlage, die allen Sicherheitsanforderungen moderner Systeme entspricht. Hier besteht die einhellige Meinung, dass Mikrokernsysteme besonders geeignet sind, sichere Systeme zu konstruieren, da sich mit ihnen das Prinzip der kleinen vertrauenswürdigen Systembestandteile (small Trusted Computing Base (TCB)) umsetzen lässt. Um das Prinzip des kleinsten Privilegs (POLA, Principle of Least Privilege) umzusetzen bedarf es jedoch einer Weiterentwicklung des L4 Systems im Ganzen: die Weiterentwicklung vom System der zweiten Generation zu einem System der dritten Generation. Die heute benutzten Systeme der dritten Generation sind capability-basiert und ermöglichen es Programmen nur die Ressourcen zur Verfügung zu stellen, die sie benötigen. Andere Ressourcen sind für das Programm weder greifbar noch sichtbar. Man spricht hier auch von einem System mit lokalen Namen, da in Capability-Systemen jedes Programm einen eigenen virtuellen Namensraum besitzt. Mit der Umstellung der Basisprimitive wurde auch eine Runderneuerung des L4Env nötig um es an die neuen Schnittstellen des capability-basierten Systems anzupassen. Das neue System ist das „L4 Runtime Environment – L4Re“.

Gleichzeitig mit der Betonung der Sicherheitseigenschaften des Systems, ohne die Echtzeiteigenschaften zu vergessen, werden Virtualisierungsfähigkeiten verlangt. Angefangen mit der x86-Architektur haben alle breit verfügbaren Architekturen ihre Fähigkeiten bezüglich Virtualisierung erweitert und erlauben es Gastsysteme effizient auszuführen. Für ein Mikrokernsystem ist die Unterstützung solcher Funktionalität essentiell um vorhandene Software sicher in das System einbinden zu können. Hier sind insbesondere die Isolationseigenschaften eines Mikrokernsystems wichtig, da sie zusichern, dass ein kompromittierter Gast keine anderen Systemkomponenten oder andere Gäste kompromittieren kann. Im Laufe der Zeit erhielt das L4Re System Unterstützung für alle Virtualisierungserweiterungen der unterstützten Architekturen (Intel, AMD, ARM und MIPS). Das L4Re System kann damit auch als Hypervisor-System bezeichnet werden.

Neben den Basisfähigkeiten einer Betriebssystemplattform wird L4Re auch zur Erforschung von Zuverlässigkeitsaspekten herangezogen. In letzter Zeit beschäftigt sich die Gruppe verstärkt mit Höchstleistungsrechensystemen und deren Ziel des „Exa-Scale“ Systems. Hier ist die Gruppe im DFG-geförderten Forschungsprojekt „FFMK“ aktiv. In zukünftigen Höchstleistungsrechensystemen sind insbesondere wieder Betriebssystemaspekte von Bedeutung, wobei der Einsatz eines Mikrokernsystems hier diverse Vorteile verspricht. Vorhandene Erfahrungen und Mechanismen aus dem Bereich der Echtzeitsysteme können hier wieder angewendet werden.

Durch weitere zahlreiche deutschland- und europaweite Projekte wurde das L4Re in verschiedenen Kontexten erfolgreich eingesetzt. Zum Beispiel ist es Basis vom „SiMKo 3“, einem Smartphone für Hochsicherheitseigenschaften, was unter Federführung der Deutschen Telekom entwickelt wurde. Dieses und weitere Projekte haben die Möglichkeit eröffnet, die L4Re Technologie aus der Universität auszugründen. Die Open-Source L4Re Plattform wird nun hauptsächlich in der Kernkonzept GmbH weiterentwickelt und zusammen mit Kunden in Produkte integriert. Die Hauptmotivation sind hier sichere und starke Isolation von Subsystemen auf einer gemeinsamen Plattform, mit der Möglichkeit durch Virtualisierung andere Systeme einzuführen, aber auch die Möglichkeit Echtzeitsysteme zu integrieren. Beispielszenarien aus den immer größer werdenden Themenkomplexen „Industrie 4.0“ und IoT sind zahlreich vorhanden.

In einem Vortrag werden wir einen Überblick über die gemachten Erfahrungen sowie über die aktuellen Entwicklungen geben.