Institut für
Systemarchitektur
Professur
Betriebssysteme

TECHNISCHE
UNIVERSITÄT
DRESDEN

µSINA
Sichere mikrokern-basierte System-architektur

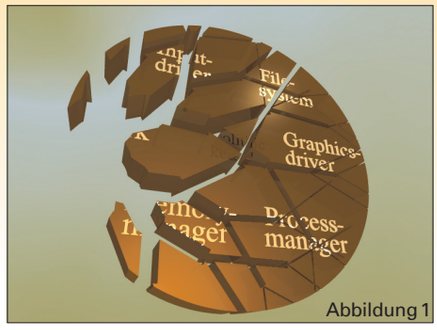

Abbildung 1

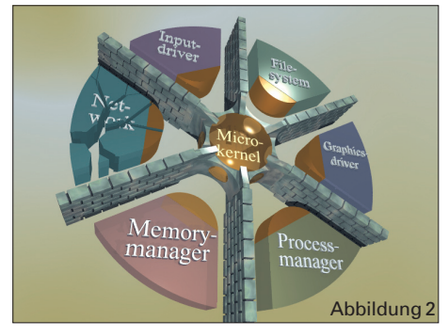

Abbildung 2

Motivation

Aktuelle Betriebssysteme müssen sehr hohe funktionale Anforderungen erfüllen. Neben der Unterstützung eines breiten Spektrums an verschiedenen Hardware-Komponenten sind für den praktischen Einsatz komplexe Software-Komponenten, z.B. Netzwerkprotokoll-Stack, Dateisysteme und Prozessverwaltung, notwendige Voraussetzung.

Mit der zunehmenden Verbreitung des Internets und der damit verbundenen globalen Vernetzung von verschiedenen Informationssystemen wird die Sicherheit der gespeicherten und übertragenen Daten zu einem der Hauptprobleme moderner IT-Systeme.

Ein Großteil der gegenwärtig eingesetzten Betriebssysteme basiert auf dem klassischen Ansatz, alle grundlegenden Systemfunktionen in ein komplexes Programm – den monolithischen Systemkern – zu integrieren. Dieser Systemkern wird im privilegierten Modus des Prozessors ausgeführt, welcher uneingeschränkten Zugriff auf alle Daten des Systems gewährt. Aus diesem Grund müssen Anwender solcher Systeme dem monolithischen Kern vollständig vertrauen. Dieses Vertrauen ist in Anbetracht der hohen Komplexität eines solchen Kerns nicht gerechtfertigt. Beispielsweise besteht ein typischer Kern des Betriebssystems Linux aus ca. 500.000 Programmzeilen.

Programmierfehler und Sicherheitslücken sind bei derart umfangreichen Softwaresystemen unvermeidlich. Fehlerhafter Programmcode kann die verlässliche Funktionsweise des gesamten Systems beeinflussen und fatale Auswirkungen haben (Abbildung 1).

Bei modernen Betriebssystemen und Hardware-Plattformen wird durch die Isolation von Anwendungen in virtuellen Adressräumen verhindert, dass sich lokale Programmfehler auf das gesamte System auswirken können. Jede Nutzerapplikation besitzt ihren eigenen Adressraum und kann nur über Kernmechanismen auf die Daten einer anderen Applikation zugreifen. Der Schutz der einzelnen Anwendungsprogramme wird durch den Systemkern realisiert.

Mikrokerne nutzen die existierenden technischen Möglichkeiten zur Kapselung aller Komponenten des Systems. Auf diese Weise lassen sich Auswirkungen von Fehlern und sicherheitskritischen Schwachstellen in den Systemkomponenten lokal begrenzen (Abbildung 2). Allen Systemkomponenten neben dem Mikrokern werden die Privilegien entzogen, da deren Funktionalität nicht an diese Privilegien gebunden ist. Durch den Einsatz eines Mikrokerns wird der Umfang des im privilegierten Modus des Prozessors ausgeführten Programmcodes um eine Größenordnung reduziert. Der von uns eingesetzte Mikrokern L4/Fiasco umfasst lediglich 15.000 Programmzeilen und enthält ausschließlich die Funktionen, die zwingend im privilegierten Modus des Prozessors ausgeführt werden müssen.

Exemplarische Umsetzung eines VPN Gateways

Durch die hohe Verfügbarkeit des Internets hat sich der Einsatz von virtuellen privaten Netzwerken (VPN) als Sicherheitstechnologie etabliert. Hierbei werden verschiedene, meist geographisch weit entfernte, private Netzwerke oder mobile Endgeräte über das Internet zu

einem virtuellen Netzwerk zusammengeschlossen. Der über das Internet übertragene Datenverkehr wird hierbei mittels kryptographischer Verfahren, die z.B. im IPSec-Standard festgelegt sind, vor unbefugter Einsichtnahme oder einer Verfälschung durch Dritte geschützt. Die Sicherung der zu übertragenen Daten obliegt dem VPN-Gateway. Es bildet die Schnittstelle vom lokalen privaten Netzwerk zum öffentlichen Internet. Für den Nutzer ist der Einsatz des VPN-Gateways vollkommen transparent.

Die IPSec-Implementierung ist Bestandteil eines monolithischen Betriebssystemkerns und eng mit anderen komplexen Netzwerkfunktionen und weiteren Kernkomponenten verknüpft. Die sicherheitskritischen Funktionen sind verglichen mit dem Rest des Kerns von geringer Komplexität und umfassen lediglich Kryptographie sowie Protokollunterstützung für IPSec.

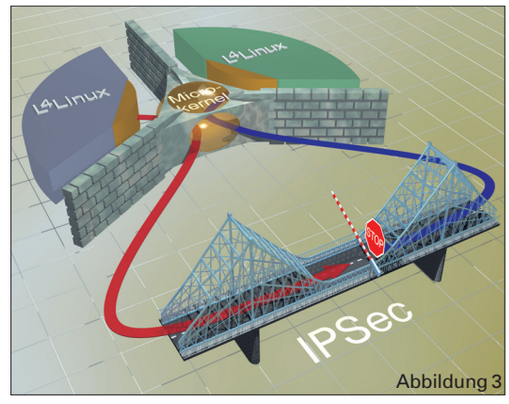

Abbildung 3

Die Mikrokerntechnologie erlaubt neben der Kapselung einzelner Systemkomponenten auch die Isolation kompletter Betriebssysteminstanzen. L4Linux ist eine Portierung von Linux auf den Mikrokern. Dem Systemkern von Linux wurden alle Privilegien entzogen, welche die Sicherheit des Systems gefährden könnten. Dabei ist L4Linux aber vollständig (binär-)kompatibel zum ursprünglichen Linux, wodurch Applikationen ohne Modifikationen ausgeführt werden können.

Die Implementierung unseres mikrokernbasierten VPN-Gateways löst die IPSec-Implementierung aus dem Systemkern von Linux heraus und lagert sie in eine eigenständige Komponente (Viaduct) aus.

Unser VPN-Gateway nutzt zwei Instanzen von L4Linux. Jede Instanz kann ausschließlich über eine dedizierte, physische Netzwerkverbindung kommunizieren. Die Netzwerkverbindungen der Instanzen sind jeweils dem privaten oder dem öffentlichen Netz fest zugeordnet. Die Kommunikation zwischen den Instanzen erfolgt ausschließlich über das Viaduct, welches für die Durchsetzung der VPN-Sicherheitspolitik verantwortlich ist (Abbildung 3).

Durch das Herauslösen der sicherheitskritischen Komponente aus dem Systemkern wird der Umfang des vertrauenswürdigen Programmcodes eines VPN-Gateways noch einmal um eine Größenordnung reduziert. Zusätzlich existiert eine klare Trennung zwischen der privilegierten Komponente (Mikrokern), der IPSec-Implementierung (Viaduct) und dem übrigen System (L4Linux). Die notwendige Kommunikation zwischen diesen Komponenten wird im Design des Systems eindeutig beschrieben und kann zur Laufzeit mittels Mechanismen des Mikrokerns kontolliert werden.

Mikrokernbasierte sichere Systemarchitektur

Am Beispiel des obigen VPN-Gateways wird deutlich, dass sich mittels der Mikrokerntechnologie sicherheitskritische Systeme in einzelne durch Adressräume von einander getrennte Komponenten aufteilen lassen, so dass die Auswirkungen eines Fehlers oder einer sicherheitskritischen Schwachstelle lokal auf diese Komponente begrenzt bleiben.

Bei der Umsetzung des VPN-Gateways wurden die Grundlagen für eine mikrokernbasierte Systemarchitektur geschaffen, so dass perspektivisch auch diverse Grundschutzrelevante IT-Sicherheitsapplikationen portiert werden können, bspw.: Firewalls, Intrusion Detection & Response Systeme, Router oder mobile Endgeräte.

Die secunet Security Networks AG wurde im Dezember 1999 seitens des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit der Entwicklung von SINA (Sichere Inter-Netzwerk-Architektur) beauftragt. SINA ist eine IT-Sicherheitsplattform für die sichere Verarbeitung, Speicherung, Übertragung und Nachweisführung von Verschlusssachen und äquivalent sensitiven Daten. Inzwischen sind mehr als 2.000 SINA-Komponenten im Einsatz, Tendenz stark steigend.

Die mittels des VPN-Gateways realisierten Basiskomponenten der sicheren mikrokernbasierten Systemarchitektur bilden voraussichtlich die technologische Grundlage für die SINA-Systemplattform der nächsten Generation. Der Einsatz der Mikrokerntechnologie würde eine einfachere Integration neuer Kernkomponenten zulassen, da die Modularisierung des Systemkerns ausschließt, dass eine neue Komponente die bereits vorhandenen Komponenten (sicherheitsfunktional) beeinflussen kann. µSINA ermöglicht dadurch die Offenheit von SINA gegenüber späteren Systemerweiterungen, was diese Sicherheitslösung für nahezu alle Branchen interessant macht.

Kooperationspartner

secunet Security Networks AG • Dr. Michael Sobirey
Ammonstraße 74 • 01067 Dresden
Tel: +49 (351) 43959-0
E-Mail: info@secunet.com • http://www.secunet.de

Bundesministerium für Wirtschaft und Arbeit

gefördert durch
das Bundesministerium für Wirtschaft und Arbeit

Kontakt

Technische Universität Dresden
Institut für Systemarchitektur
Prof. Hermann Härtig
Hans-Grundig-Str. 25 • 01307 Dresden
Fon +49 351 463-39438
Fax +49 351 463-38284
E-Mail: mikrosina@os.inf.tu-dresden.de
http://os.inf.tu-dresden.de/mikrosina/