NOVA und Bastei - Neue Ansätze Mikrokernel-basierter Systeme

Stefan Kalkowski (TU-Dresden)

7. Oktober 2007

Die Betriebssystem-Gruppe der TU-Dresden befasst sich seit längerem mit verschiedenen Aspekten Mikrokernel-basierter Systeme, wie insbesondere Sicherheit[10][7][6], Echtzeitfähigkeit[9][8][4] und Virtualisierung[5][2] bestehender Betriebssysteme und darauf laufender Software.

Aktuell wird im Rahmen des ROBIN-Projekts[1] an einer verbesserten Koexistenz von existierenden Betriebssystemen und einer Multi-Server Umgebung, auf Basis des neu entwickelten Hypervisors **NOVA**, gearbeitet. Die Multi-Server Umgebung **Bastei** wurde ebenfalls von Grund auf neu konzipiert und ist das vorläufige Ergebnis von zehn Jahren Forschung unserer Betriebssystem-Gruppe auf diesem Gebiet. In diesem Vortrag soll die Arbeit der TUD-Betriebssystem-Gruppe im Rahmen des ROBIN Projekts vorgestellt werden.

1 NOVA

Die NOVA OS Virtualization Architecture umfasst einen im Kernel-Modus laufenden, minimalen Hypervisor, sowie eine Virtual-Machine-Monitor Komponente, die im nicht-priviligierten Modus läuft. Mittels NOVA können unmodifizierte, vorhandene Betriebssysteme innerhalb virtueller Maschinen direkt neben Echtzeit- und sicherheitskritischen Anwendungen ausgeführt werden. Hierbei werden zur verbesserten Performance die neuen Virtualisierungsfunktionen derzeitiger x86 Plattformen ausgenutzt. NOVA wurde von Beginn an auf eine vereinfachte formale Verifikation hin entwickelt[11].

2 Bastei

Die Aufteilung vormals monolithischer Betriebssystemkerne in einen Mikrokern einerseits und mehrere, separierte Komponenten andererseits, sowie die Anforderung die *Trusted Computing Base* einer jeden Anwendung möglichst klein zu halten, um deren Sicherheit zu erhöhen, wirft die Frage auf, wie diese Komponenten zu gestalten und anzuordnen sind, um die gegenseitigen Abhängigkeiten minimal zu halten. Diese Frage versucht das C++ Framework Bastei[3] mittels einiger weniger, vorgegebener Komponenten und Protokolle zu beantworten.

Darüberhinaus versucht Bastei, neben herkömmlichen Zugriffs-Kontroll-Schutz-Mechanismen für die Gewährleistung von Vertraulichkeit und Integrität, durch "die Bezahlung" von Serverdiensten *Denial of Service* -Attacken zu begegnen. Die dezentrale Anordnung von Sicherheitspolitiken erlaubt ausserdem eine vereinfachte Administration auch komplexerer Systeme. Die Verwendung lokaler Namensräume ermöglicht die Re-Konfiguration bestehender Systeme ohne Komponenten neu übersetzen oder verlinken zu müssen.

Literatur

[1] Robin project web page, October 2007.

[2] Robert Baumgartl, Martin Borriss, Hermann Härtig, Michael Hohmuth, and Jean Wolter. Linux-Portierung auf den Mikrokern L4. *Wissenschaftliche Beiträge zur Informatik*, (1), 1996. In German.

[3] Norman Feske and Christian Helmuth. Design of the Bastei OS architecture. Technical Re-

port TUD-FI06-07-Dezember-2006, TU Dresden, 2006.

[4] H. Härtig, R. Baumgartl, M. Borriss, Cl.-J. Hamann, M. Hohmuth, F. Mehnert, L. Reuther, S. Schönberg, and J. Wolter. DROPS: OS support for distributed multimedia applications. In *Proceedings of the Eighth ACM SIGOPS European Workshop*, Sintra, Portugal, September 1998.

[5] Hermann Härtig, Michael Hohmuth, and Jean Wolter. Taming Linux. In *Proceedings of the 5th Annual Australasian Conference on Parallel And Real-Time Systems (PART '98)*, Adelaide, Australia, September 1998.

[6] C. Helmuth, A. Westfeld, and M. Sobirey. μSINA - Eine mikrokernbasierte Systemarchitektur für sichere Systemkomponenten. In *Deutscher IT-Sicherheitskongress des BSI*, volume 8 of *IT-Sicherheit im verteilten Chaos*, pages 439–453. Secumedia-Verlag Ingelsheim, May 2003.

[7] Hermann Härtig, Michael Hohmuth, Norman Feske, Christian Helmuth, Adam Lackorzynski, Frank Mehnert, and Michael Peter. The nizza secure-system architecture., 2005.

[8] F. Mehnert, M. Hohmuth, and H. Härtig. Cost and benefit of separate address spaces in real-time operating systems. In *Proceedings of the 23rd IEEE Real-Time Systems Symposium (RTSS)*, pages 124–133, Austin, Texas, USA, December 2002.

[9] Martin Pohlack, Ronald Aigner, and Hermann Härtig. Connecting real-time and non-real-time. Technical report, Technical University of Dresden, February 2004.

[10] Lenin Singaravelu, Calton Pu, Hermann Haertig, and Christian Helmuth. Reducing tcb complexity for security-sensitive applications: Three case studies, April 2006.

[11] Henrik Tews, Bart Jacobs, Erik Poll, Marko van Ekelen, and Peter van Rossum. Specification and verification of the nova microhypervisor. Technical report, Raboud Universiteit Nijmegen, 2007.