TECHNISCHE
UNIVERSITÄT
DRESDEN

Faculty of Computer Science / Institute of Systems Architecture / Operating Systems

Less is More
A Secure Microkernel-based OS

Adam Lackorzynski, Alexander Warg

TECHNISCHE
UNIVERSITÄT
DRESDEN

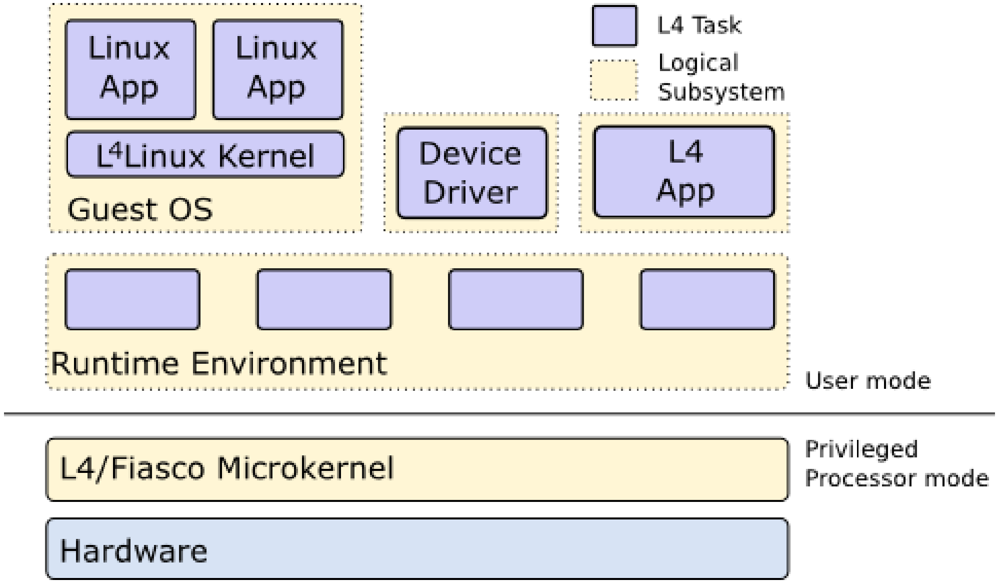
OS Research at TU Dresden

Group

- since 1993
- About a dozen people

Research

- Microkernels
- Microkernel-based OS
- Resource Management
- Legacy (VM) support



- Security Properties / Isolation
- Real-Time Properties
- Robustness / Resilient Computing
- Multi-Core Architectures

- Formal Verification

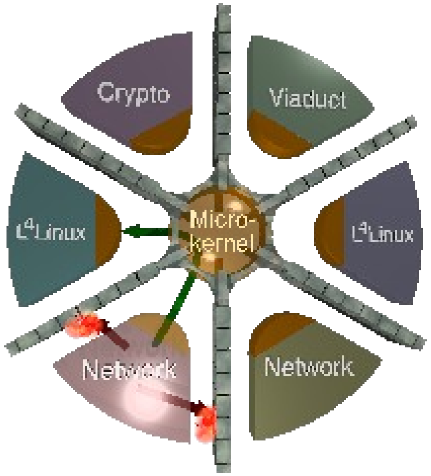
Sandboxing — OS Design

Google Chrome

- Improve security, use processes for tabs
- Processes of a single user are weakly isolated

µ-kernel OS

- Small secure OS kernel (in privileged mode)
- *Strongly isolated processes* — replace global name-spaces (e.g., UNIX-FS) by *object-capability model*
- Use processes for file systems, device drivers, OSes...
- Virtual-Machines for of-the-shelf OSes (Android...)



VPFS — Virtual Private File System

- Encapsulation and tunneling to build a secure file system

Outlook

- Software Fault Tolerance in operating systems
- Combine security sensitive and real-time workloads
- Platform- and Power-Management in component based system (multi-VM systems)
- Quantitative and functional analysis and modeling of µ-kernel OS (QuaOS)

»Wissen schafft Brücken.«