Deutsche Forschungsgemeinschaft

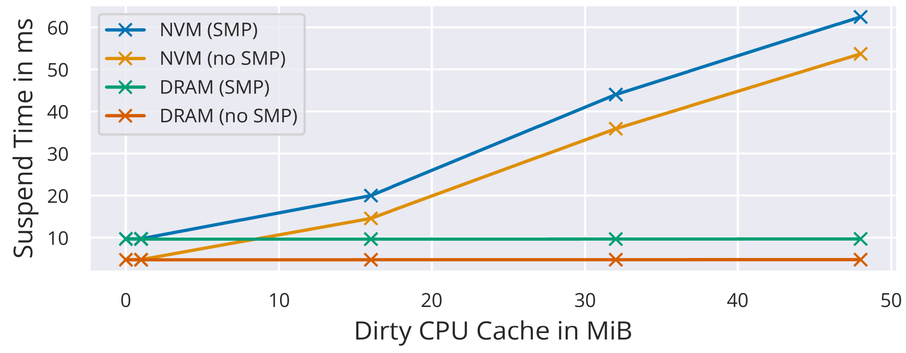
barkhausen institut

Phase 1: Fossil – Operating System Support to Leverage Byte Granular NVM Technologies

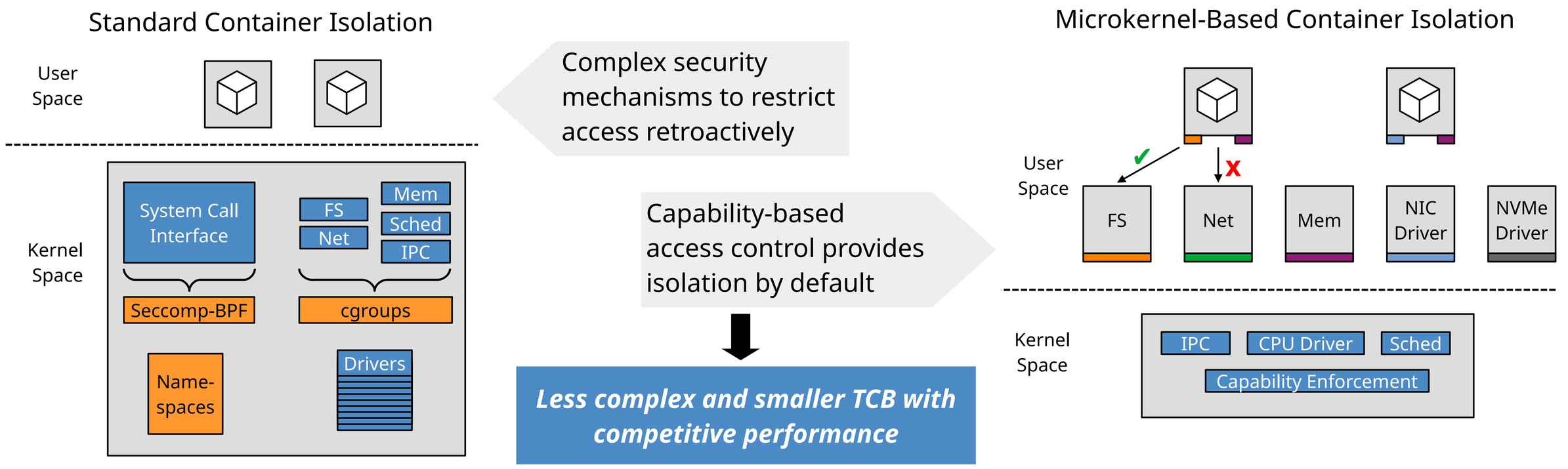
Till Miemietz, Michael Roitzsch, and Hermann Härtig

An NVM Performance Study Towards Whole System Persistence on Server Platforms [DIMES'23]

- Extended L4Re microkernel with notion of NVM
- Flush volatile state triggered by power-fail interrupt
- Check for existing system state in NVM during boot



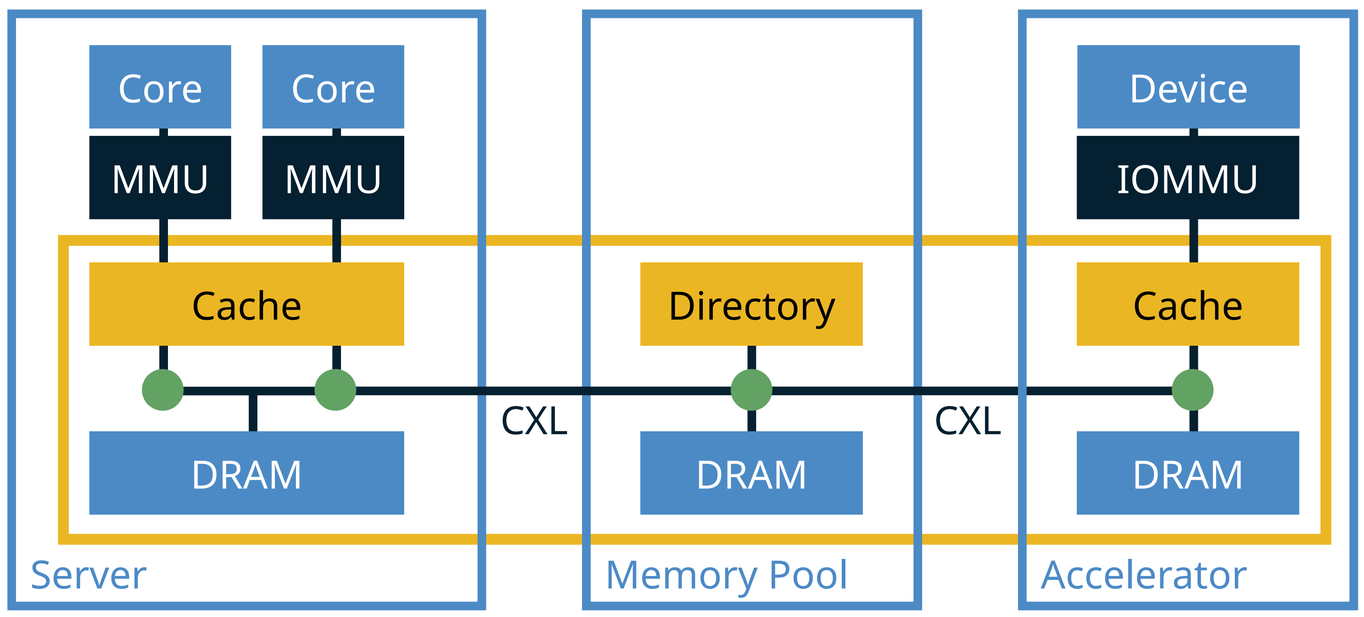
MettEagle: Costs and Benefits of Implementing Containers on Microkernels [OSDI'25]



Phase 2: ccFossil – Secure Cache Coherence for Disaggregated Memory

Matthias Hille, Michael Roitzsch, and Hermann Härtig

CXL – A Successor to NVM



- CXL requires trust in all fabric-attached devices
- Existing protection mechanisms work on virtual addresses → CXL works on physical addresses

Proposal: Selective Cache-Coherence

- Dimension 1:
  Restrict coherence to a subset of nodes
- Dimension 2:
  Restrict coherent address ranges

Approach

- Add new protection components
- Integrate HW in M3 platform (gem5 & FPGA)
- Transfer results to CXL fabrics

Research Questions

- How to configure secure selective cache-coherence in the OS?
- How to build hardware to support secure selective cache-coherence?
- What is the impact of CXL-based fabrics on the trust model of TEEs?