seL4 Update
Foundation and TS R&D News

Gernot Heiser
Chairman, seL4 Foundation
Leader, Trustworthy Systems, UNSW Sydney

gernot@sel4.systems
seL4 Foundation Update
Great success
- In Munich, hosted by HENSOLDT Cyber
- 91 attendees
  - 70/70 in-person (38 members, 17 non-members, 7 hobbyists, 8 students)
  - 21 remote
- 2 keynotes, 14 talks, 6 talks+discussions, 3 experience reports, 3 overviews
  1 AMA, 1 Panel, 4 BoFs, 6 training/tutorials
- 3 industry sponsors: DornerWorks, Horizon, Xcalibyte
**5th seL4 Summit: Minneapolis, Sep’23**

- In Minneapolis, USA
- 19–21 Sep 2023
- High number of proposals received
- Preliminary program out about 22 May
News

After a year of upheaval and growth, now a year of consolidation

- seL4 Trademark – registered in US and China
- new members: NCSC, LatticeX, Google, SpacemiT, Autoware (and 3 departures)

Community support

- overhaul of Endorsement scheme: only services
- strategic investment in community support, project seed funding

Technical progress

- new kernel fastpaths: Notification signalling and VM exceptions
- verification of MCS, AArch64 progressing
- on-going work on Rust support
- a number of new platforms supported
And the Most Exciting News is...

seL4 wins the 2022 ACM Software System Award

AWARDS & RECOGNITION
Software System Award Goes to Fourteen for the Development of Groundbreaking High-Performance Operating System

Gernot Heiser, University of New South Wales; Gerwin Klein, Proofcraft; Harvey Tuch, Google; Kevin Elphinstone, University of New South Wales; June Andronick, Proofcraft; David Cock, ETH
R&D at Trustworthy Systems
OS Framework: seL4 Core Platform

- Thin wrapper of seL4 abstractions
- Encourage “correct” use of seL4
- Software development kit eases development

Simple, event-driven programming model
High-Performance I/O on seL4CP

- Lightweight, highly modular design
- Simple, event-based, single-threaded drivers
- Asynchronous, zero-copy transport layer using lock-free, bounded SPSC queues

![Diagram of IP Stack, Control region, and Driver with numbered elements: 2, 3, 3, 3, 1, 4, 1, 4]
Device Sharing
Device Sharing with Legacy Re-Use
Comparison to Linux

Linux:
- NW driver: 4k lines
- NW system total: 1M lines

seL4-based “KISS” design:
- NW driver: 700 lines
- MUX: 400 lines
- Copier: 200 lines
- IP stack: much simpler, client library
- shared NW system total: < 2,000 lines

Written by second-year student!
How About Performance?

Simplicity wins!

Gigabit Ethernet

Throughput (Mb/s)

CPU Utilization (%)

Load (Mb/s)

Linux Xput

KISS Xput

CPU

CPU

Smaller is better

Bigger is better

TC-CoE Summit, May'23

seL4 Foundation and R&D Update – © Gernot Heiser 2023 – CC BY 4.0
How About Correctness?

**KISS design:**
- NW driver: 700 lines
- MUX: 400 lines
- Copier: 200 lines
- IP stack: much simpler, client library
- shared NW system total: < 2,000 lines

Simple, sequential, event-driven code

Can apply automated verification techniques!
seL4CP Verification

Conditions apply

CapDL spec

First release within weeks!

SDF Spec

Compiler/Linker

system.elf

PD1.c

PD2.c

libsel4cp.c

f(){
  ...
}
f(..);

TC-CoE Summit, May'23

seL4 Foundation and R&D Update – © Gernot Heiser 2023 – CC BY 4.0
Plans for the (Near) Future

OS for IoT/cyberphysical systems, built on seL4CP+sDDF

Taking sDDF design principles to the complete OS:
- Fine-grained modularity, strong separation of concerns
- Radical Simplicity™: provide only the features needed
- Swappable, use-case specific policy (rather than universal policy)
- Performant
- Verifiable

- SMT solvers for components
- Model-checking for interactions

TC-CoE Summit, May’23

seL4 Foundation and R&D Update – © Gernot Heiser 2023 – CC BY 4.0