The seL4® Foundation
Growing Through Upheaval

Gernot Heiser
Chair, seL4 Foundation

gernot@sel4.systems
What is seL4?
Background: What is seL4?

seL4 is an open source, high-assurance, high-performance operating system microkernel

- Available on GitHub under GPLv2 license
- World’s most comprehensive mathematical proofs of correctness and security
- World’s fastest microkernel
- Piece of software that runs at the heart of any system and controls all accesses to resources

![Diagram showing software and hardware partitioning with critical, non-critical, and untrusted components, and an attack arrow]
What is **seL4**?

seL4 is the most trustworthy foundation for safety- and security-critical systems

Already in use across many domains:
- automotive
- aviation
- space
- defence
- critical infrastructure
- cyber-physical systems
- IoT
- industry 4.0
- certified security...
Unique Verification by Mathematical Proof

Confidentiality  Integrity  Availability

Security Enforcement

Arm 32b  RISC-V 64b

Abstract Model  Functional Correctness  C Implementation

Translation Correctness  Binary code

Arm 32b  x86 64b  RISC-V 64b

Proofs are machine-checked, using interactive theorem proving (translation correctness fully automated)

Presently unverified:
- boot code
- details of MMU, caches
- multicore

seL4: Still only capability-based OS kernel with correctness proof!

seL4: World’s first OS kernel with correctness proof!
... and Performance

Latency (in cycles) of a round-trip cross-address-space IPC on x64

<table>
<thead>
<tr>
<th>Source</th>
<th>seL4</th>
<th>Fiasco.OC</th>
<th>Zircon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mi et al, 2019</td>
<td>986</td>
<td>2717</td>
<td>8157</td>
</tr>
<tr>
<td>Gu et al, 2020</td>
<td>1450</td>
<td>3057</td>
<td>8151</td>
</tr>
<tr>
<td>seL4.systems, Nov’20</td>
<td>797</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Still the world’s fastest microkernel!

Sources:
- Zeyu Mi, Dingji Li, Zihan Yang, Xinran Wang, Haibo Chen: “SkyBridge: Fast and Secure Inter-Process Communication for Microkernels”, EuroSys, April 2020
- Jinyu Gu, Xinyue Wu, Wentai Li, Nian Liu, Zeyu Mi, Yubin Xia, Haibo Chen: “Harmonizing Performance and Isolation in Microkernels with Efficient Intra-kernel Isolation and Communication”, Usenix ATC, June 2020
- seL4 Performance, [https://sel4.systems/About/Performance/](https://sel4.systems/About/Performance/), accessed 2020-11-08

Temporary performance regression in Dec’19
A Microkernel is not an OS

All operating-system services are user-level processes:
- file systems
- device drivers
- power management
- virtual machines
- ...
“Capabilities” Control Communication

No communication unless explicitly authorised!
Brief seL4 History

- 05–09: developed and implementation correctness proved at NICTA (Arm-32)
- 11–13: proofs of binary correctness, security enforcement, worst-case latencies
- Jul’14: open sourced (GPLv2)
- Jul’15: Boeing ULB helicopter flying autonomously on seL4
- Apr’17: DARPA HACMS final demos showing seL4 defeating cyber attacks
- ≈ 2018: shipped in defence products
- Apr’20: seL4 Foundation created under Linux Foundation
- Jun’20: implementation correctness proved for RISC-V
- May–Dec’21: RISC-V proofs of binary correctness and security enforcement
- Aug’21: DARPA “steal this drone” challenge at DEFCON, all attacks defeated
The seL4 Foundation
What Happened in May’21?

Innovation Oz Style: CSIRO believes a secure kernel and kicked out of the house. CSIRO believes a secure kernel and kicked out of the house.

China, Singapore has dumped CSIRO self-driving car project.

Dumped CSIRO team gets funding lifeline from UNSW.

The research team behind the extremely hard-to-hack microkernel sel4 has received lifeline funding to the end of the year from the University of New South Wales. The team, known as Trustworthy Systems at the CSIRO, was sensationally dumped by the agency earlier this month as part of a restructure that will see up to 70 jobs cut.

The new funding from UNSW School of Computer Science and Engineering will allow most of the Trustworthy Systems team — more than a dozen at the CSIRO and a
Life After CSIRO
On Life Support (UNSW Bridge Funding)
What Happened to TS People?

Core Trustworthy Systems seL4 Team

Jan'20: 38 people
- CSIRO, 34
- UNSW, 4

Jan'21: 26 people
- CSIRO, 21
- UNSW, 5

Jan'22: 22 people
- UNSW, 22

Since Sep’21:
strongest influx of new talent in 5–10 years!

People movements
- Retained, 13
- Lost, 10
- Community, 10
- New, 9
What’s Behind This Development?

- CSIRO’s abandonment triggered a spill of developers into the community
  - Upside: less organisational dependence, broadening of developer base
  - Downside: loss of experience at TS
    - being compensated (with delay) by strong inflow of students
- Without UNSW support, TS would be completely dispersed
  - would be hard to rebuild, might have been fatal for seL4
  - gave us the buffer needed to rebuild funding pipeline
- Broadening developer base resulting from
  - TS people moving into community
    - in the past leaving TS usually meant leaving community
  - Industrial adoption is leading to more independent skills development
    - It seems most “other” contributors doing it as part of their job
Community Growth

Pull Requests

Prior to April’21, TS committed to internal Bitbucket
Community Growth

People submitting PRs

- TS
- former TS
- Other

Why So Few PRs?

**seL4 is a verified, high-performance microkernel!**

- Approx 10–15 kSLOC
- Strong design principles: policy-free, performance-focussed
- Verification

**Contributors must understand implications!**
Success rates of “External” PRs

Non-TS Contributors

- Merged or approved
- Closed unmerged
- Open

Let’s Talk Money
Putting Foundation $$ to Work

Possible 2022 Budget

- Community support: 39%
- Development: 19%
- Foundation Admin: 16%
- Sysadmin (UNSW): 13%
- LF tax: 9%
- LF services: 4%

Linux.conf.au, Jan'22
Gernot Heiser: The seL4 Foundation – growing through upheaval
2022 Budgets in Comparison

- **Emerging Industry Consortium**: 81%
- **TS@UNSW**: 15%
- **seL4 Foundation**: 4%
... and Community
Main Take-Aways

- Dependence on a single organisation is dangerous
  - Main motivation for setting up the seL4 Foundation
  - Must be complemented with broadening developer base
  - For now, CSIRO dependence replaced by (more benign) UNSW dependence

- seL4 has become critically important for many organisations
  - … who are prepared to support it
  - … including allied governments!

- Communication is important but difficult
  - smell of death vs encouragement to contribute back

- Media presence helps – to attract top students
Implications: Development and Engagement

Old Model

Focus on kernel

TS Research

Public $$

TS Deployment

Insights

New Model

Kernel & System

TS Research

Insights

Industry $$

Kernel verification: Proofcraft

Platform, user-mode, tools

Industry Deployment
What’s Next for seL4?
Community & Deployment Growth

Community development

Scaling up training

Entice "lost" people back

Industry to develop secure car OS

Fund AArch64 & multicore verification
Research: Keep Redefining the State of the Art

Device virtualisation

Verified time Protection:
Eliminate timing channels

Provably secure
general-purpose OS

Verified device
drivers

Verified mapping from
system spec to
code

Automated verification
of systems code

Verified real-time
guarantees

seL4 performance
improvements

D

R
Summary

- CSIRO’s abandonment was a near-death experience for seL4
- Survived thanks to UNSW support and the community rallying behind us
- Now in a stronger position than before:
  - strong support from UNSW
  - strong support from industry
  - strong support from various governments
  - growth of developer base
  - strong influx of high-achieving students into UNSW research team
- Main challenge is number of qualified people
  - scaling up development
  - scaling up research

Please join us!

https://sel4.foundation
https://sel4.systems
https://github.com/seL4/
https://microkerneldude.org/
Questions?