The seL4® Report

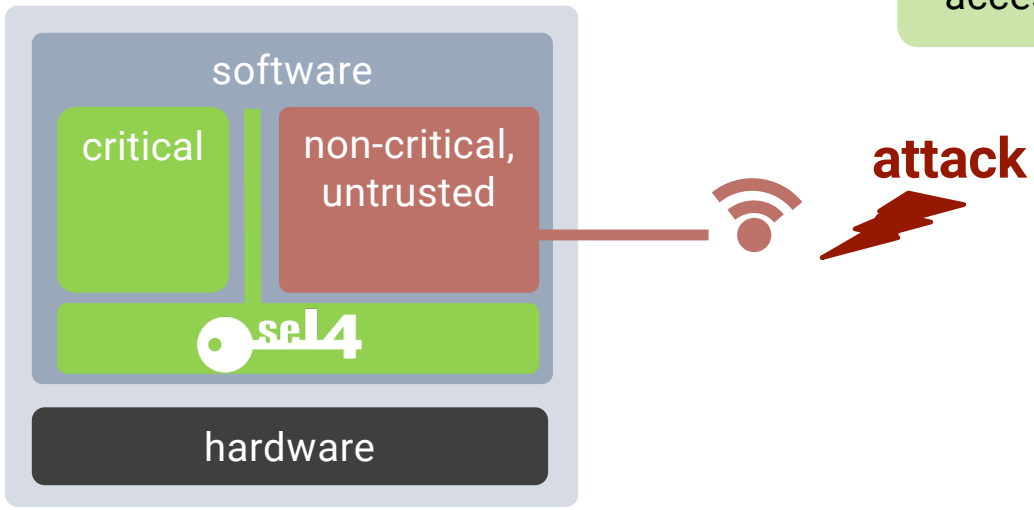
aka **State of the seL4 Ecosystem**

Gernot Heiser
Trustworthy Systems @ UNSW
Chairman, seL4 Foundation
gernot@sel4.systems

Background: What is seL4?

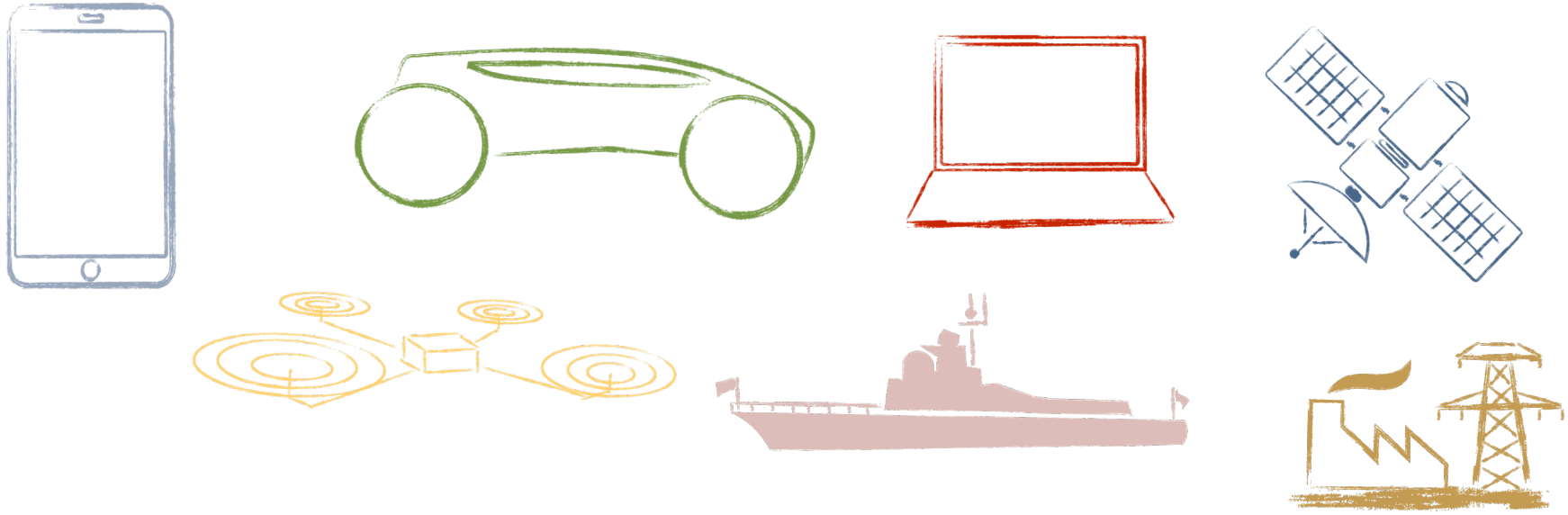
seL4 is an open source, high-assurance, high-performance operating system microkernel

- 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



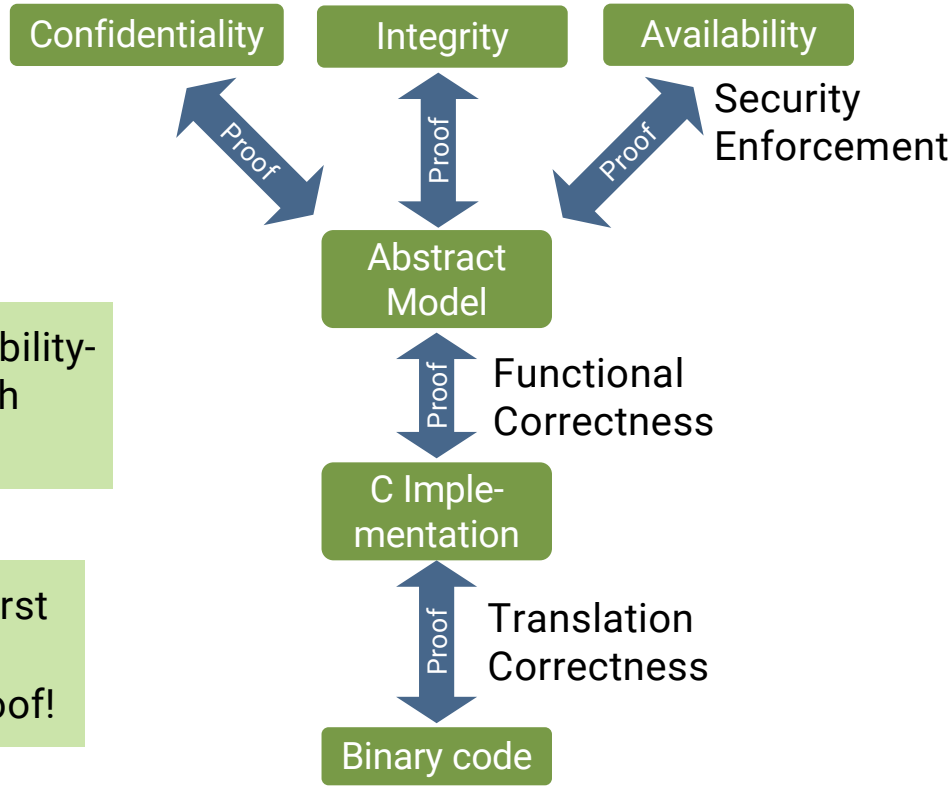
What is seL4?

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



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

seL4: World's first OS kernel with correctness proof!

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

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

Brief seL4 History – 2009–2020

- 05–09: seL4 developed and **implementation correctness** proved at NICTA (Arm-32)
- Aug'11: proof of **integrity enforcement**
- Nov'11: sound & complete **worst-case execution-time (WCET) analysis**
- May'13: proof of **confidentiality enforcement** (information flow)
- Jun'13: proof of **translation correctness** (functional correctness to binary)
- 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
- Jul'18: proof of functional correctness for 64-bit x86
- ≈ 2018: shipped in defence products
- Apr'20: seL4 Foundation created under Linux Foundation
- Jun'20: proof of **implementation correctness on RISC-V**

World First!

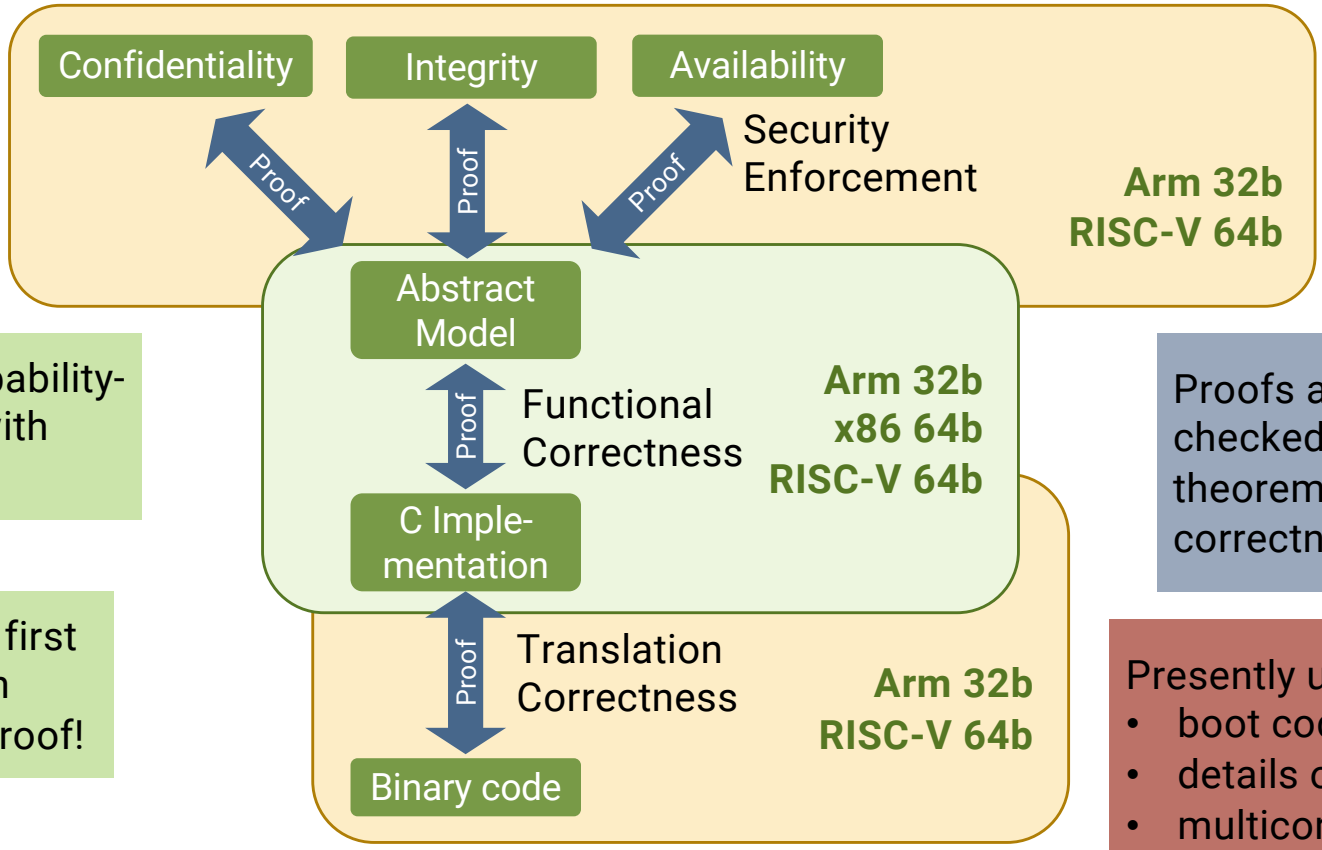
seL4 over the past 15 months

seL4 Progress Since Last seL4 Summit (Nov'20)

- May'21: proof of **translation correctness for RISC-V**

- Jun–Jul'21: strong growth of seL4 Foundation membership
- Jul'21: proof of **integrity enforcement for RISC-V**
- Aug'21: DARPA "steal this drone" challenge at DEFCON, *all attacks defeated*
- Dec'21: proof of **confidentiality enforcement for RISC-V**
- Jan'22: first refinement (of two) of MCS kernel functional correctness

Unique Verification by Mathematical Proof



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

seL4: World's first OS kernel with correctness proof!

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

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

seL4 Progress Since Last seL4 Summit (Nov'20)

- May'21: proof of **translation correctness for RISC-V**
- May'21: CSIRO abandons Trustworthy Systems Group
- Jun–Jul'21: strong growth of seL4 Foundation membership
- Jul'21: proof of **integrity enforcement for RISC-V**
- Aug'21: DARPA "steal this drone" challenge at DEFCON, *all attacks defeated*
- Dec'21: proof of **confidentiality enforcement for RISC-V**
- Jan'22: first refinement (of two) of MCS kernel functional correctness

What Happened in May'21?

ZDNet Videos Executive Guides Mobility Security NBN CXO

MUST READ: Your cybersecurity training needs impr

Innovation Oz Style: secure kernel and ki

CSIRO believes a secure kernel h all in on artificial intelligence.

Written by **Chris Duckett**, APAC Editor
Posted in Null Pointer on June 7, 2021 | Topic: Security

InnovationAus
PUBLIC POLICY AND BUSINESS INNOVATION

Home About News Podcasts See What You Can Be InnovationAus Awards

Post-COVID19 Recovery

Csiro

China, Singapore l dumped CSIRO seL

Joseph Brookes
Senior Reporter
24 May 2021

The world-leading Australian week is in the acquisition sigh Government's R&D agency.

The two potential buyers have Trusted Systems team respon

Best fitness deals 2022: $400 off Peloton Bike, $100 off Fitbit smartwatches

Best Peloton alternative 2022: Your next exercise bike

InnovationAus
PUBLIC POLICY AND BUSINESS INNOVATION

Home About News Podcasts See What You Can Be InnovationAus Awards

Post-COVID19 Recovery

Research

Dumped CSIRO team gets funding lifeline from UNSW

Joseph Brookes
Senior Reporter
31 May 2021

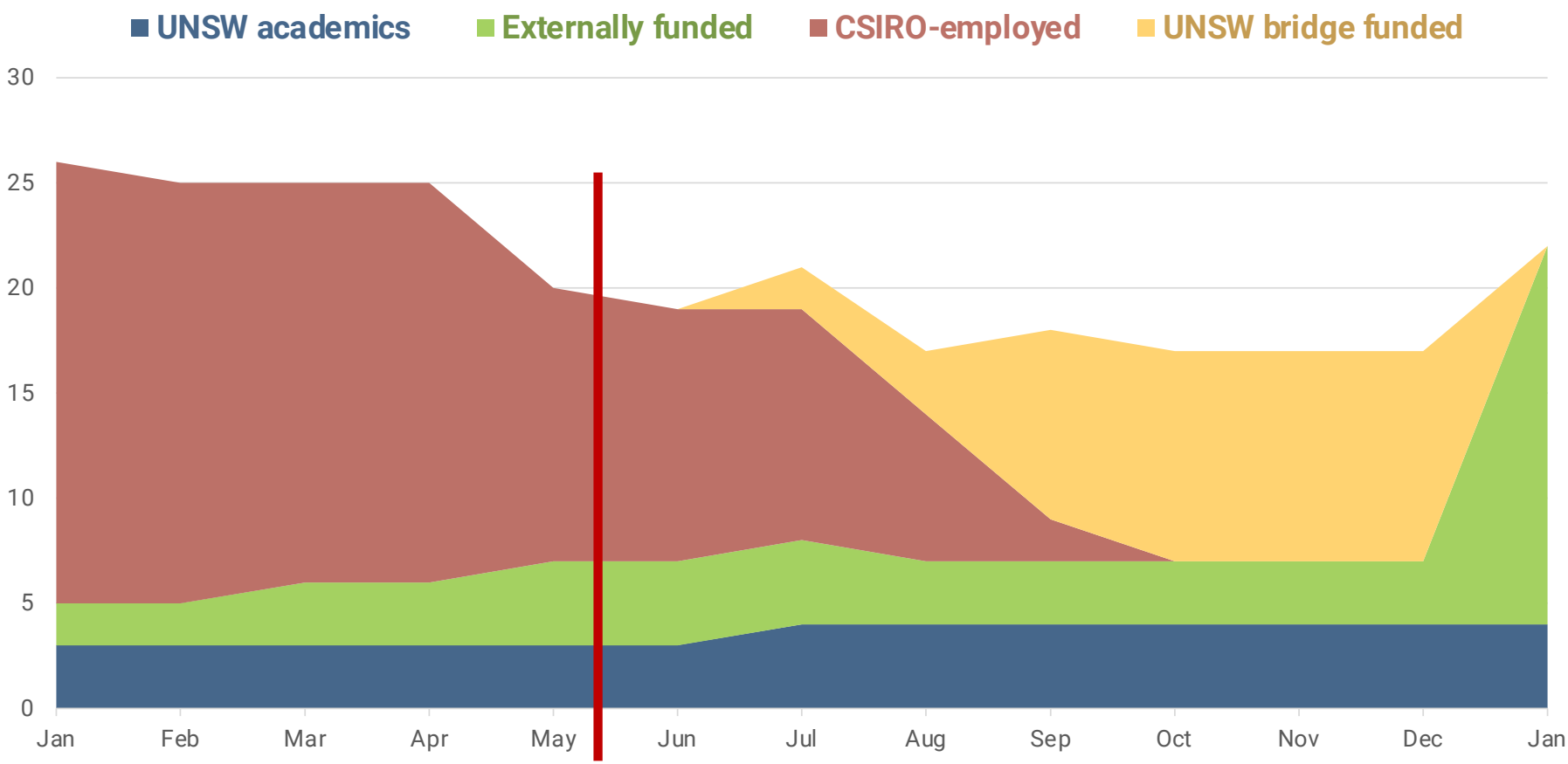
The research team behind the extremely hard-to-hack microkernel seL4 has received lifeline funding to the end of the year from the University of New South Wales. The team, known as Trustworthy Systems at the CSIRO, was sensationally dumped by the agency earlier this month as part of a restructure that 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

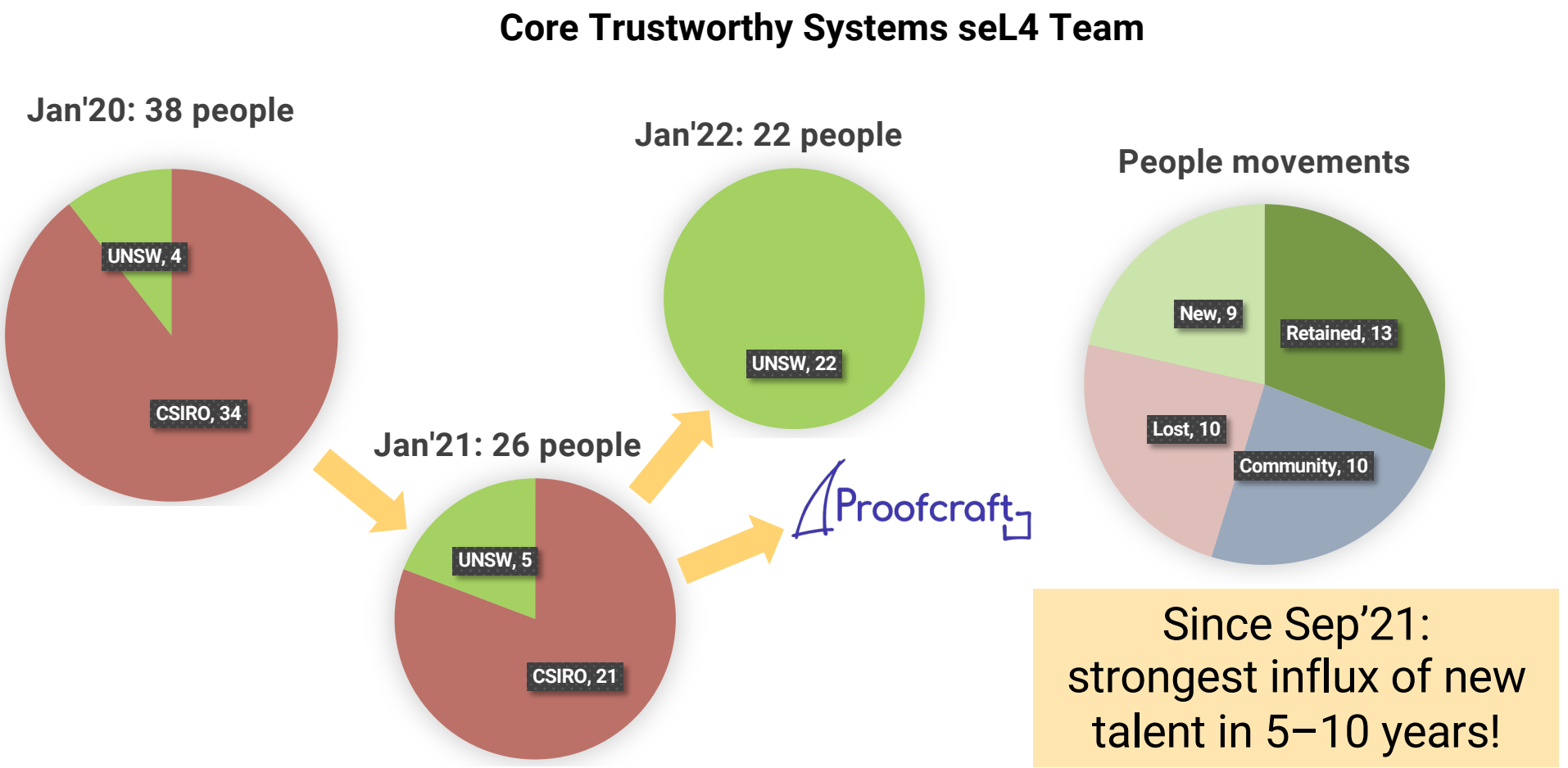
Trustworthy Systems

Life after CSIRO

2021: On Life Support (UNSW Bridge Funding)



What Happened to TS People?



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

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 seL4 contributors doing it as part of their job

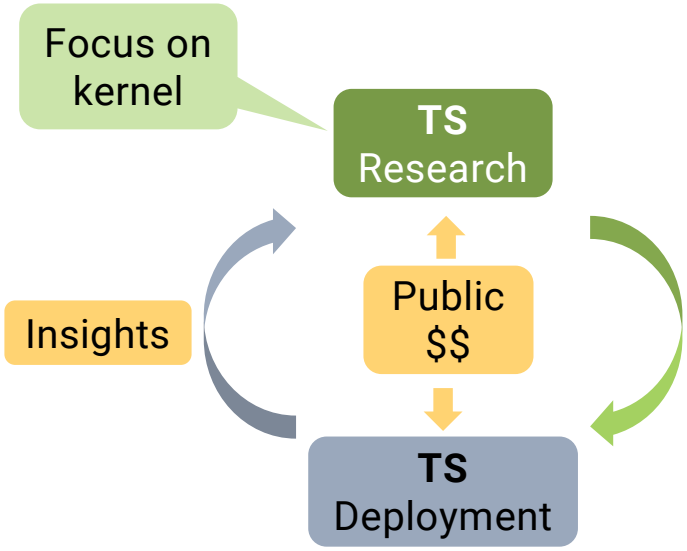
Let’s talk Community

Main Take-Aways

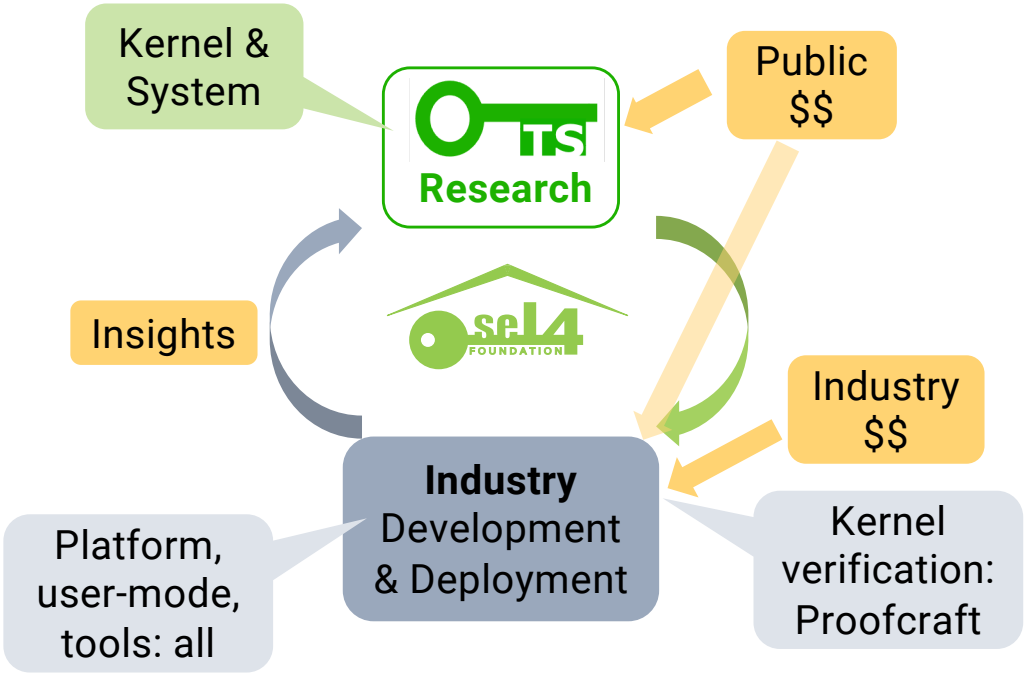
- Dependence on a single organisation is dangerous
  - Main motivation for setting up the seL4 Foundation
  - Must be complemented with broadening developer base
- seL4 has become critically important for many organisations
  - … who are prepared to support it
  - … including multiple governments!
- seL4 no longer tied to single organisation
  - TS is still critically important, but at UNSW autonomy is not threatened
- Communication is important but difficult
  - smell of death vs encouragement to contribute back
- Media presence helps – to attract top students as well as funders

Implications: Development and Engagement

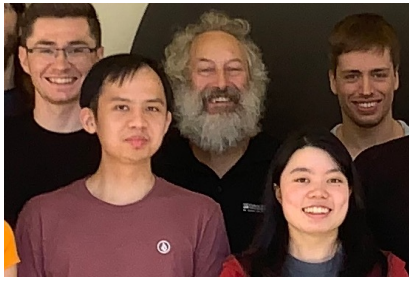
Old Model: Mostly TS



New Model: Community



Community & Deployment Growth



Develop & support community

Scale up training

Entice "lost" people back

Industry

Fund development

Fund research

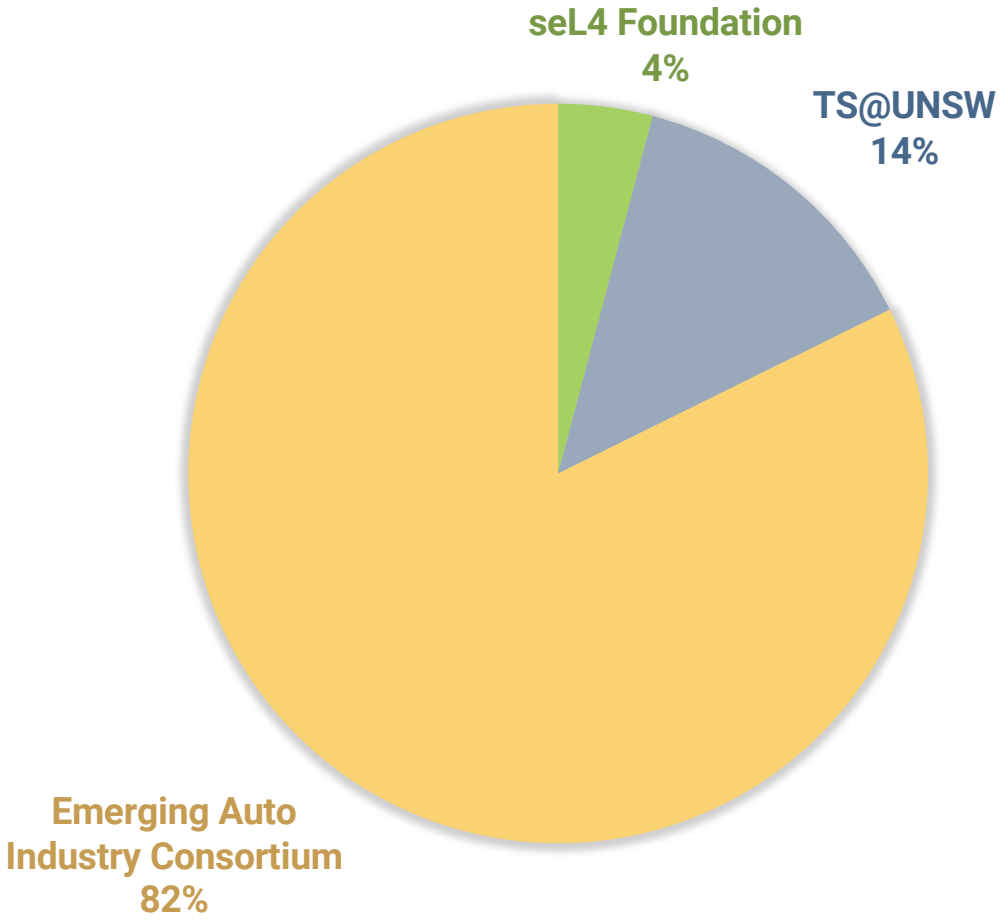
Government

& other univ. (eventually)

Drive research

Train people

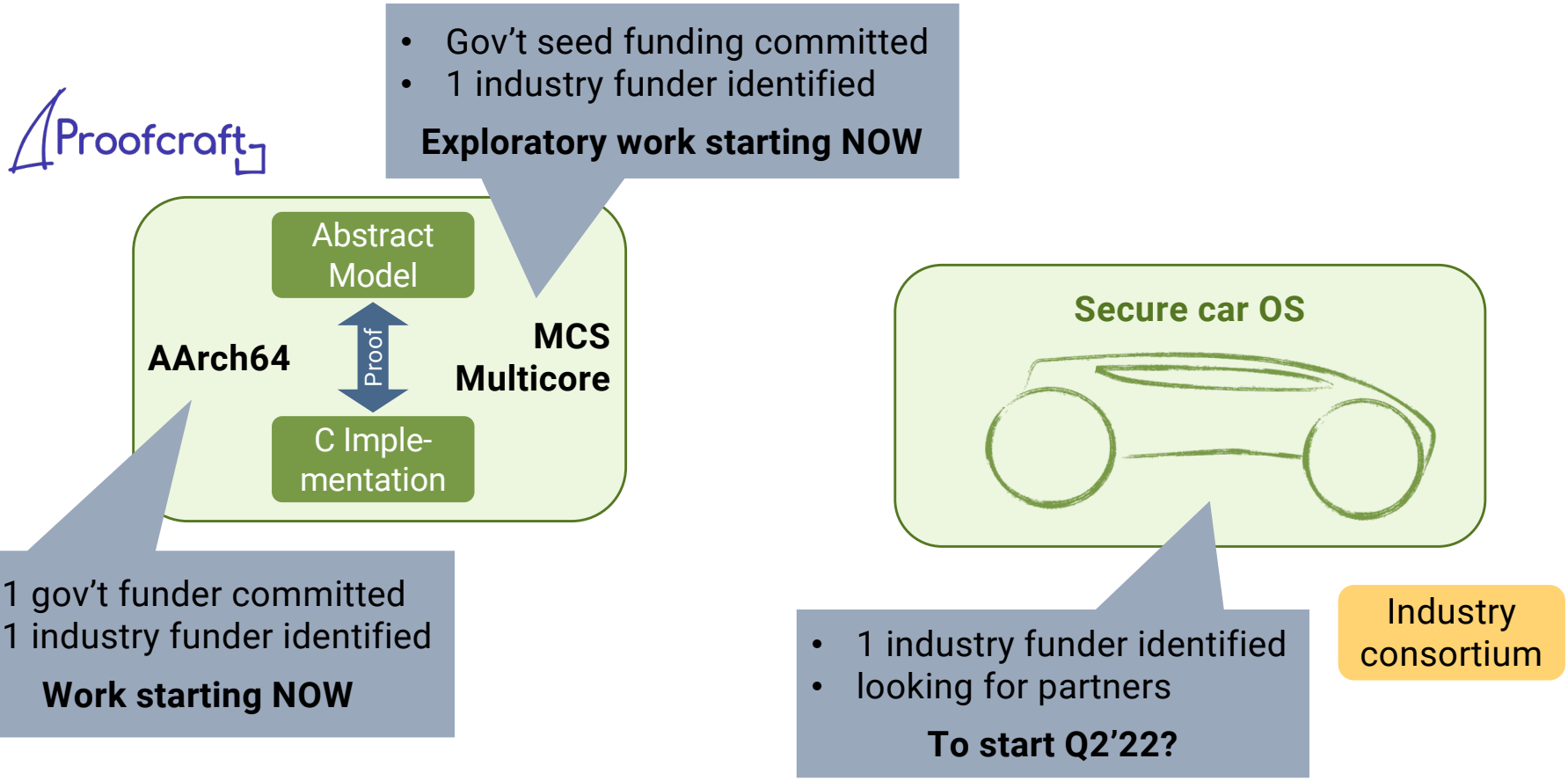
2022 Budgets in Comparison



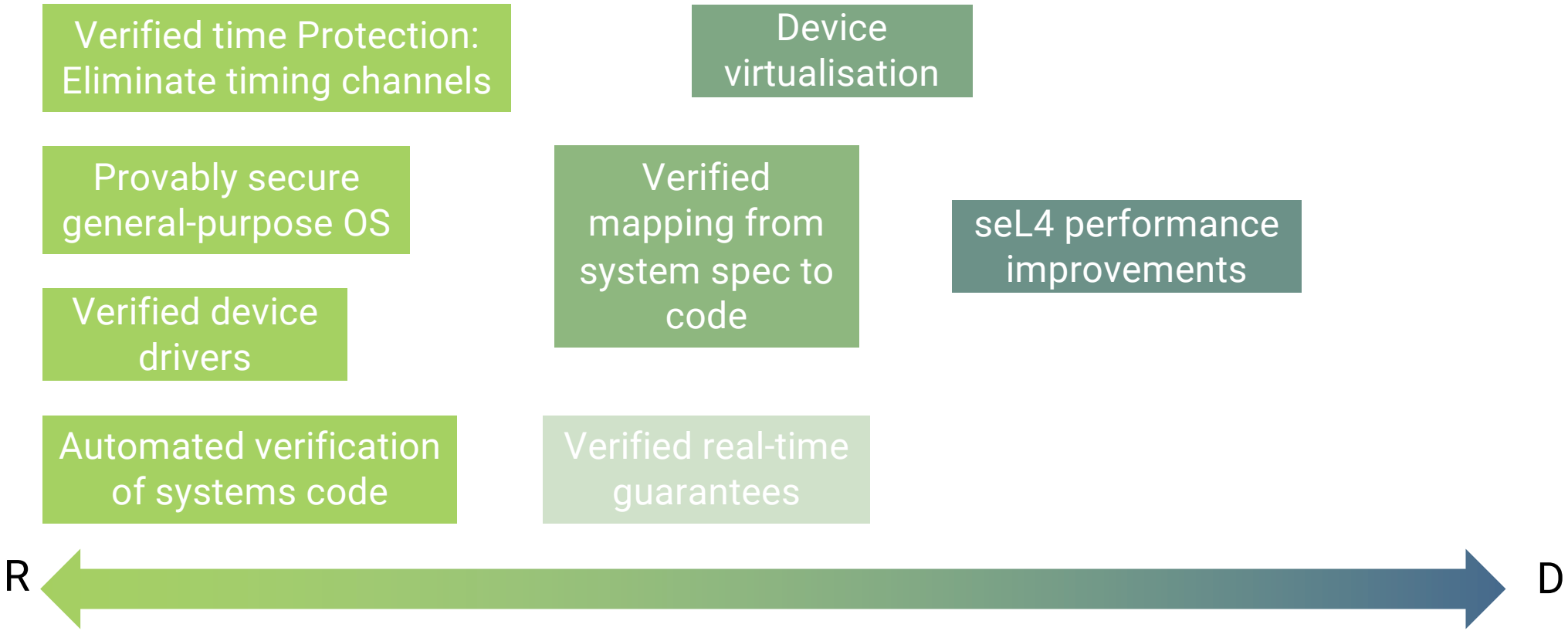
Likely dwarfed by many defence and industry developments I'm not involved in!

What’s Next for seL4?

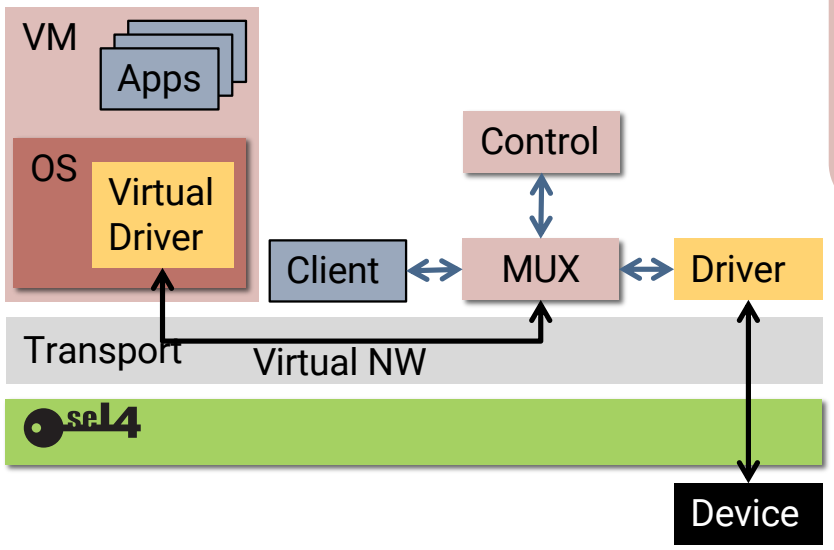
Industry: Engineering / Development



TS: Research – Keep Redefining the State of the Art



Device Virtualisation



Problem:
- Secure, low-overhead sharing of devices between VMs
- Presently ad-hoc approaches, high overheads

Solution:
- zero-copy transport layer
- standard interfaces, VirtIO
- optionally use Linux drivers in per-device VM
- investigate verifying MUX, Controller

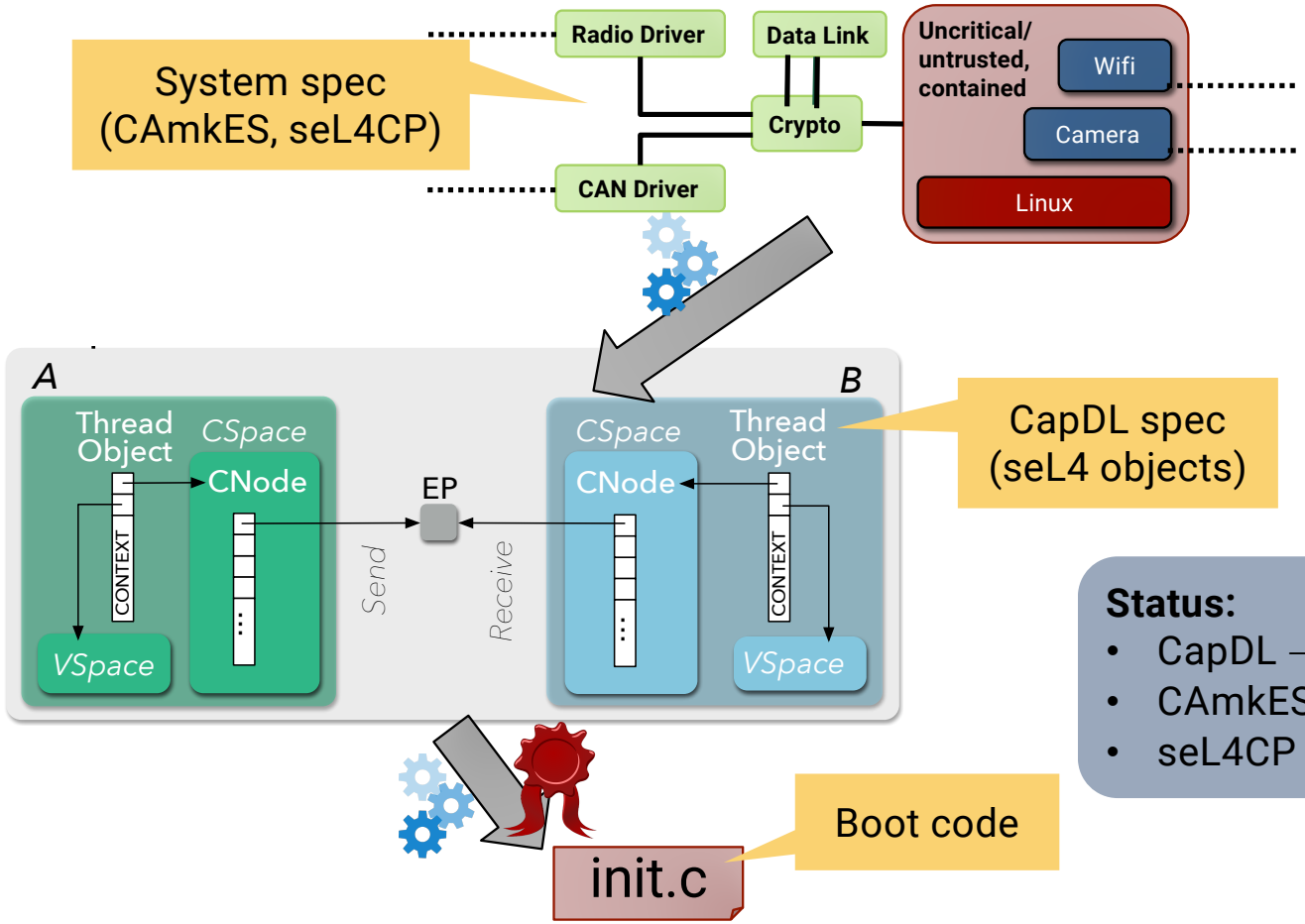
Status:
- just started

Support

TII Technology Innovation Institute

TBA (gov't org)

Verified Mapping from System Spec to Code



Aim:

- Assure mapping to enable security reasoning at system-spec level

Approach:

- Verify result state matches spec

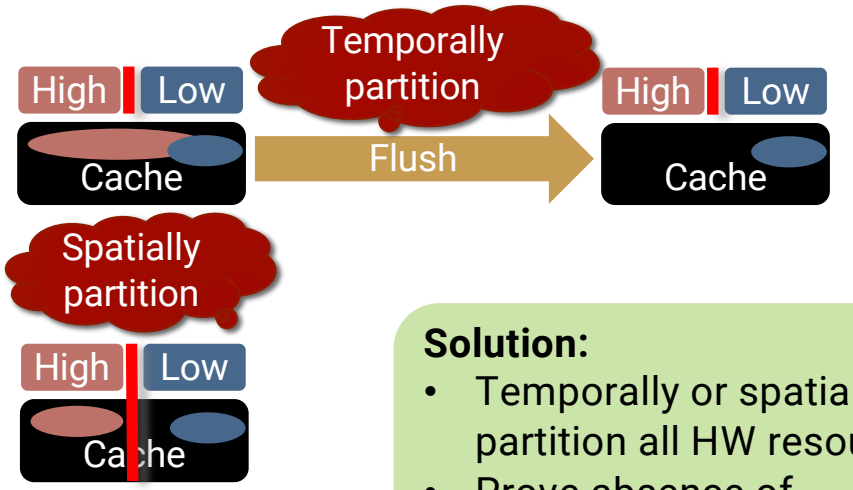
Status:

- CapDL → init code done
- CAmkES → CapDL partial
- seL4CP → CapDL starting

Support

TBA (gov't org)

Verified Time Protection



Problem:

- Competition for limited microarchitectural hardware resources creates timing channels

Solution:

- Temporally or spatially partition all HW resources
- Prove absence of information flow

Status:

- formalised hardware state
- proved abstract infoflow
- working on integrating with seL4 proofs

Support

Australian Research Council

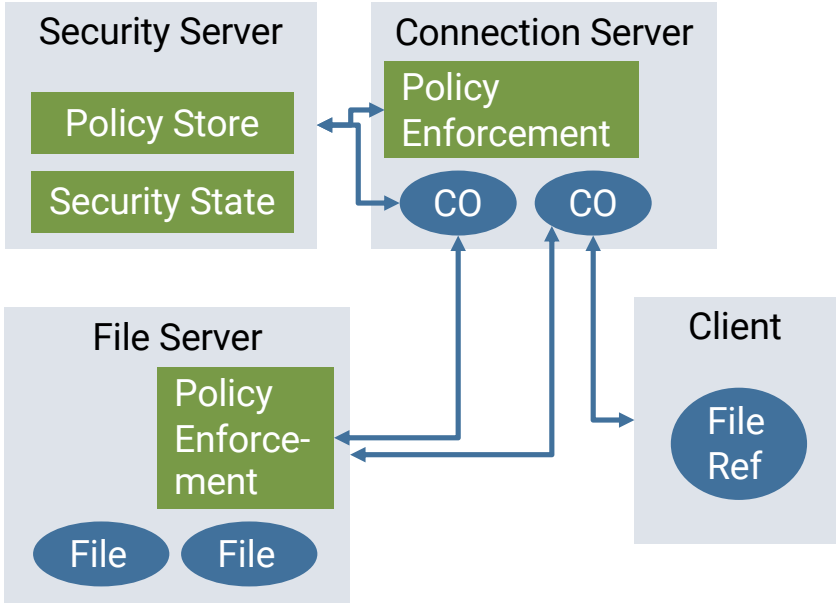
USAF-AOARD

TBA (gov't org)

Provably Secure General-Purpose OS

Aim:
- GP-OS with security policy diversity
- Proof that policy is enforced
- Performance

Approach:
- Multi-server OS with policy isolated in security server
- Object servers provable to ensure complete mediation
- Connection server authorises comms channels



Status:
- just started

Partners

Penn State

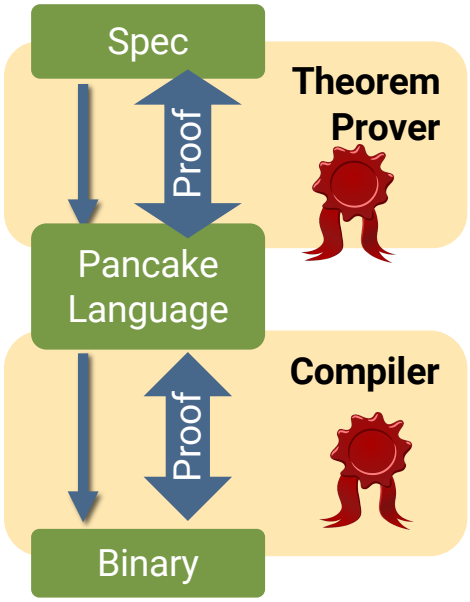
Support

TBA (gov't org)

Verified Device Drivers

Problem:
- Drivers are buggy
- Some drivers are trusted

Solution:
- Memory-safe language ***Pancake***
- Certifying compiler, derived from CakeML
- Explore generating code from high-level spec



Partners

Australian National University

Chalmers University

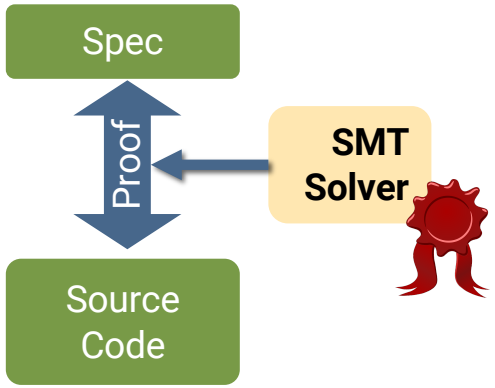
Status:
- exploratory work

Support

TBA (gov't org)

Automated Verification of Systems Code

Problem:
- Need verified drivers, NW stacks, file systems
- Manual verification (ITP) doesn't scale to full OS



Solution:
- Use SMT solvers for "push-button" verification

Status:
- exploration

Support

TBA (gov't org)

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

https://sel4.foundation
https://sel4.systems
https://trustworthy.systems/
https://microkerneldude.org/

Questions?