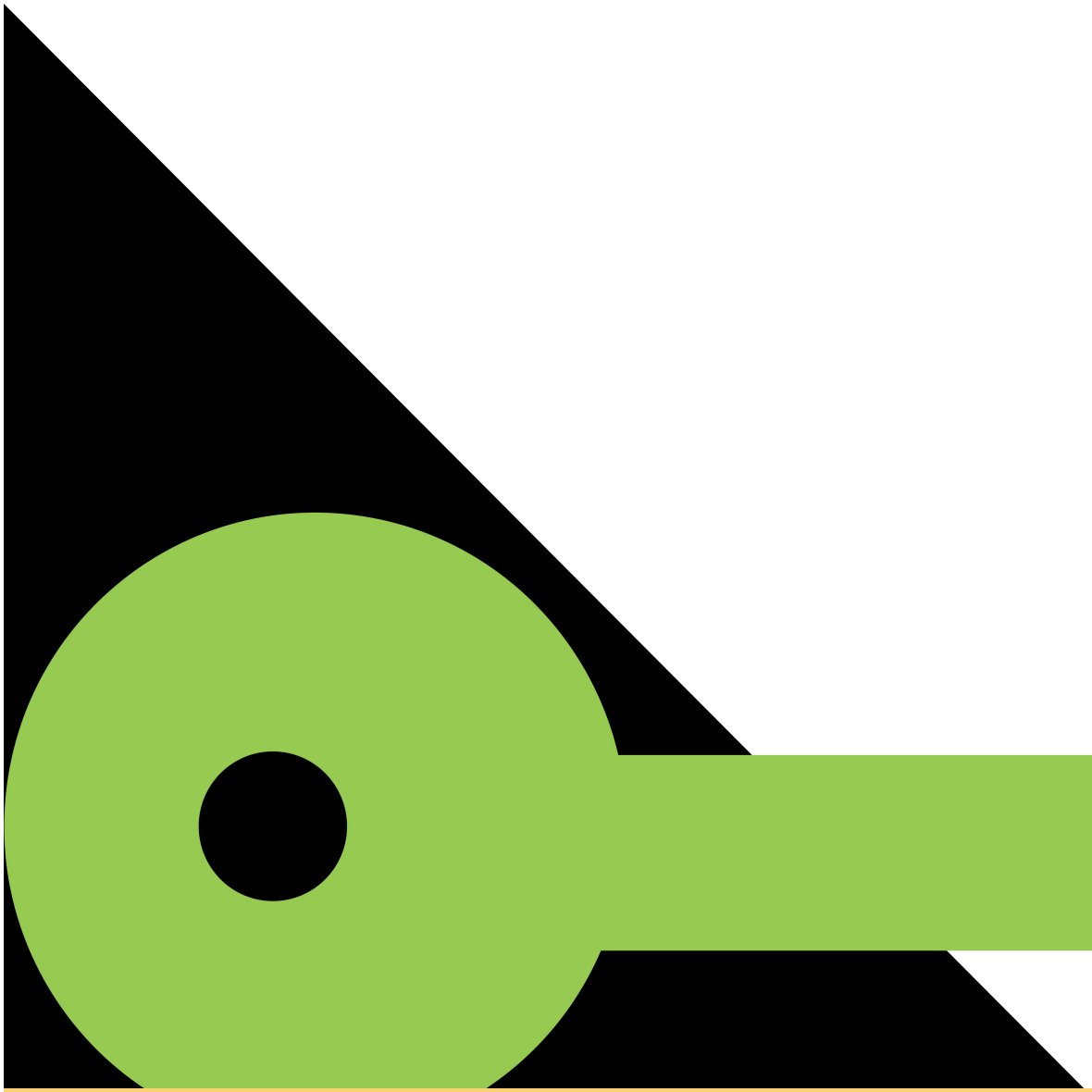


The seL4® Foundation

Growing Through Upheaval

Gernot Heiser
Chair, seL4 Foundation

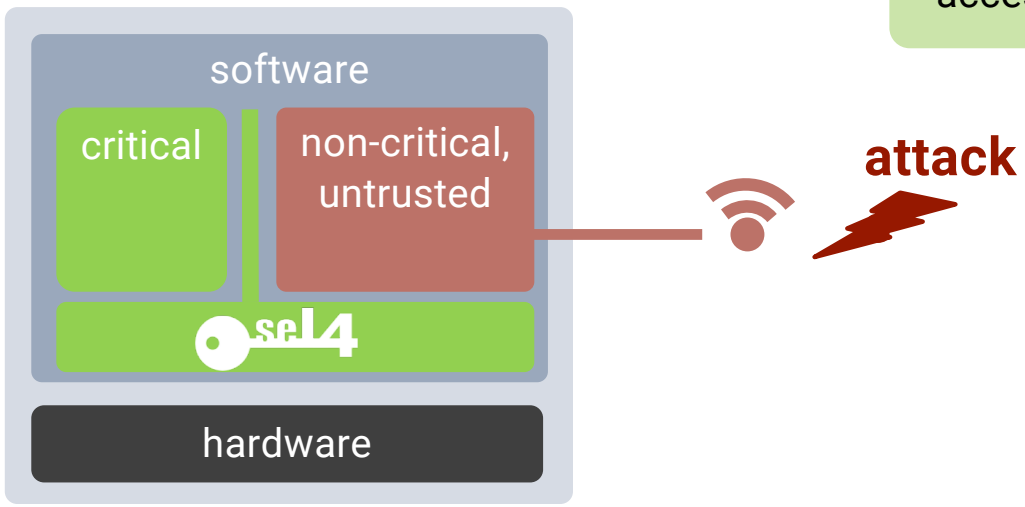
gernot@sel4.systems

What is seL4?

Background: What is seL4?

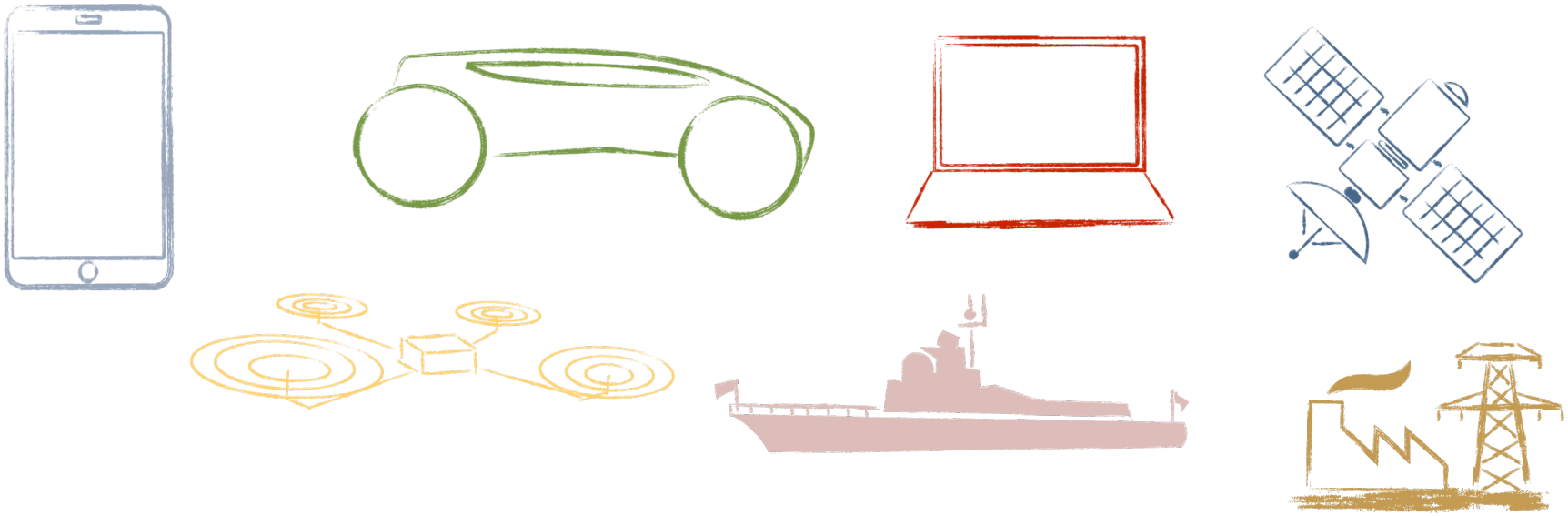
seL4 is an open source, high-assurance, high-performance operating system microkernel

- 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



What is seL4?

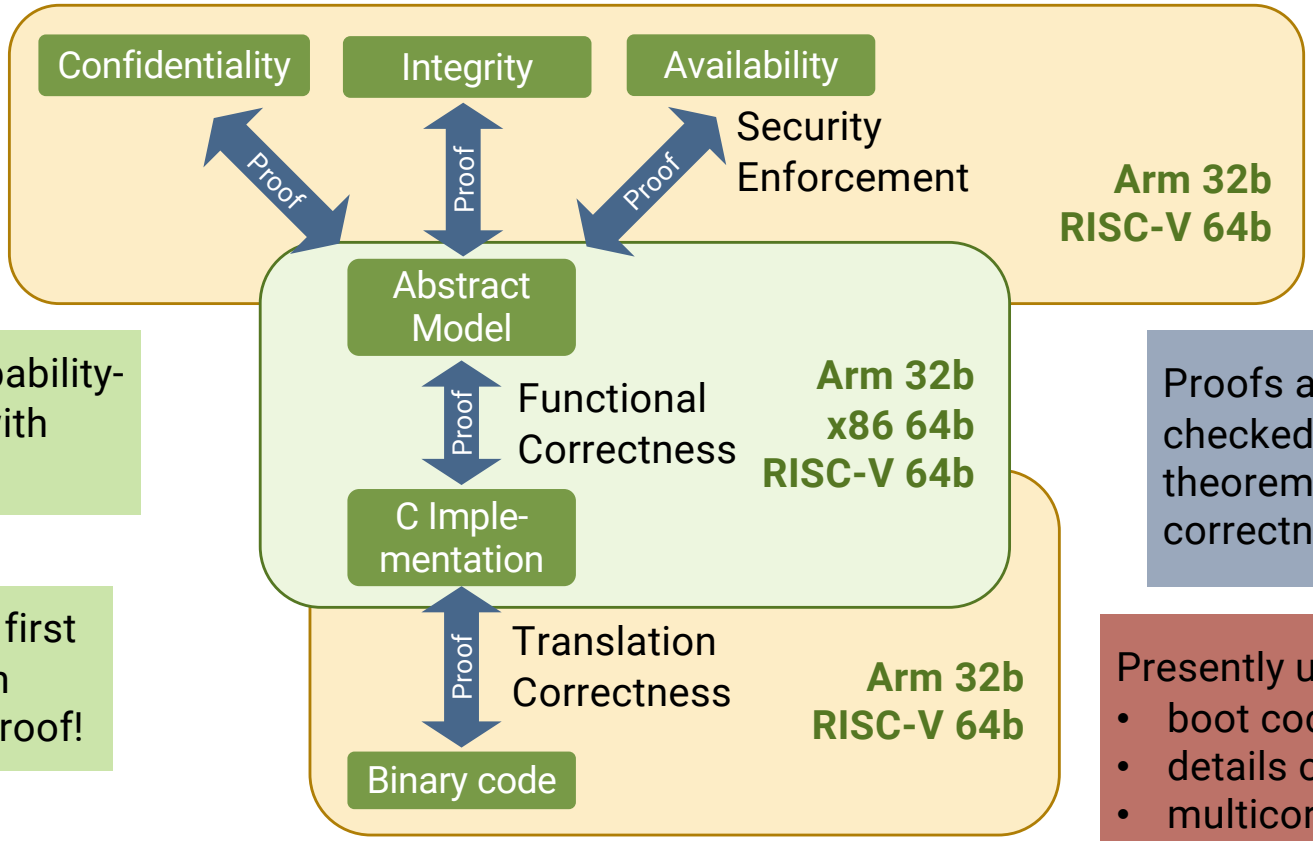
seL4 is the most trustworthy foundation for safety- and security-critical systems



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

… and Performance

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

Source	seL4	Fiasco.OC	Zircon
Mi et al, 2019	986	2717	8157
Gu et al, 2020	1450	3057	8151
seL4.systems, Nov'20	797	N/A	N/A

Still the world's fastest microkernel!

Temporary performance regression in Dec'19

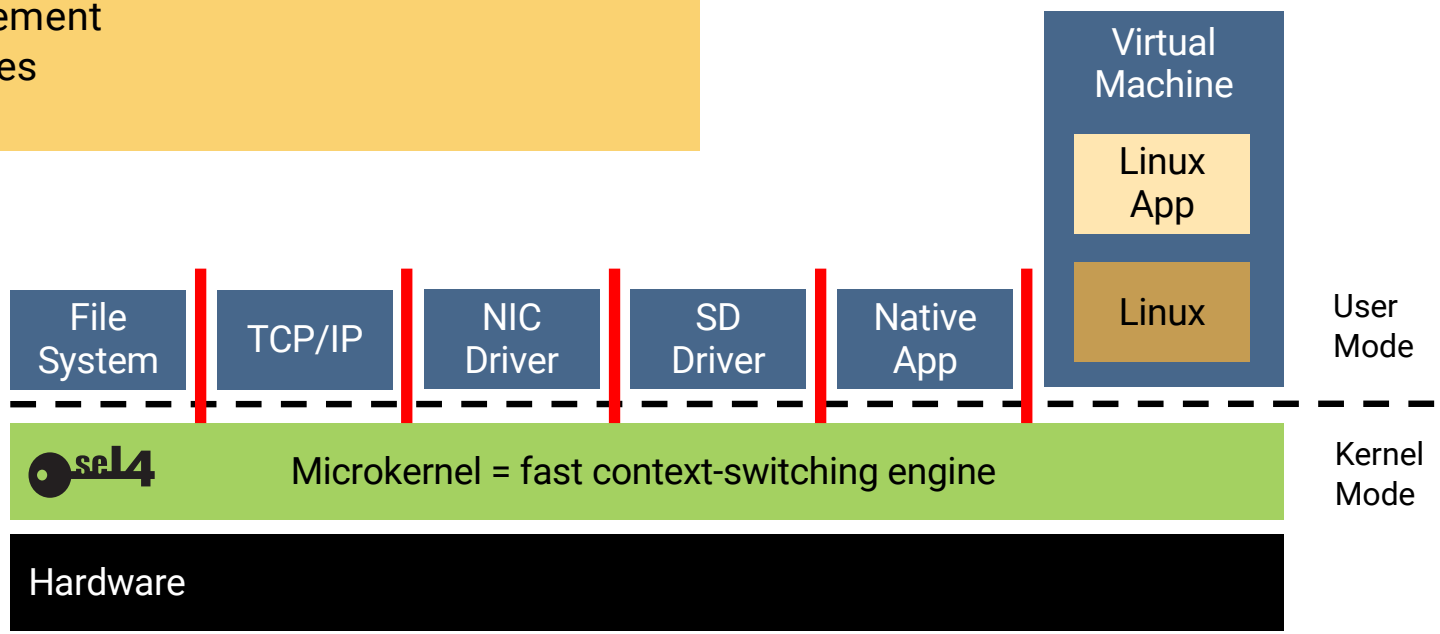
Sources:

- 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/, accessed 2020-11-08

A Microkernel is not an OS

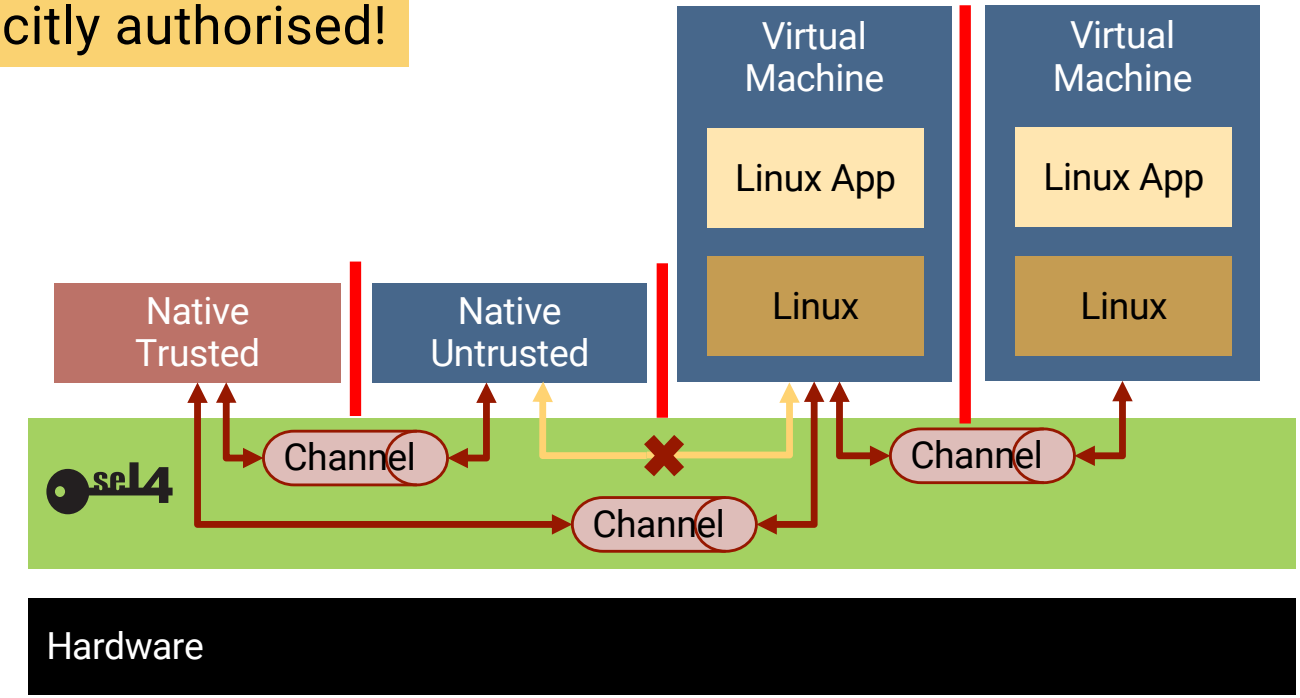
All operating-system services are user-level processes:

- file systems
- device drivers
- power management
- virtual machines
- …



“Capabilities” Control Communication

No communication
unless explicitly authorised!

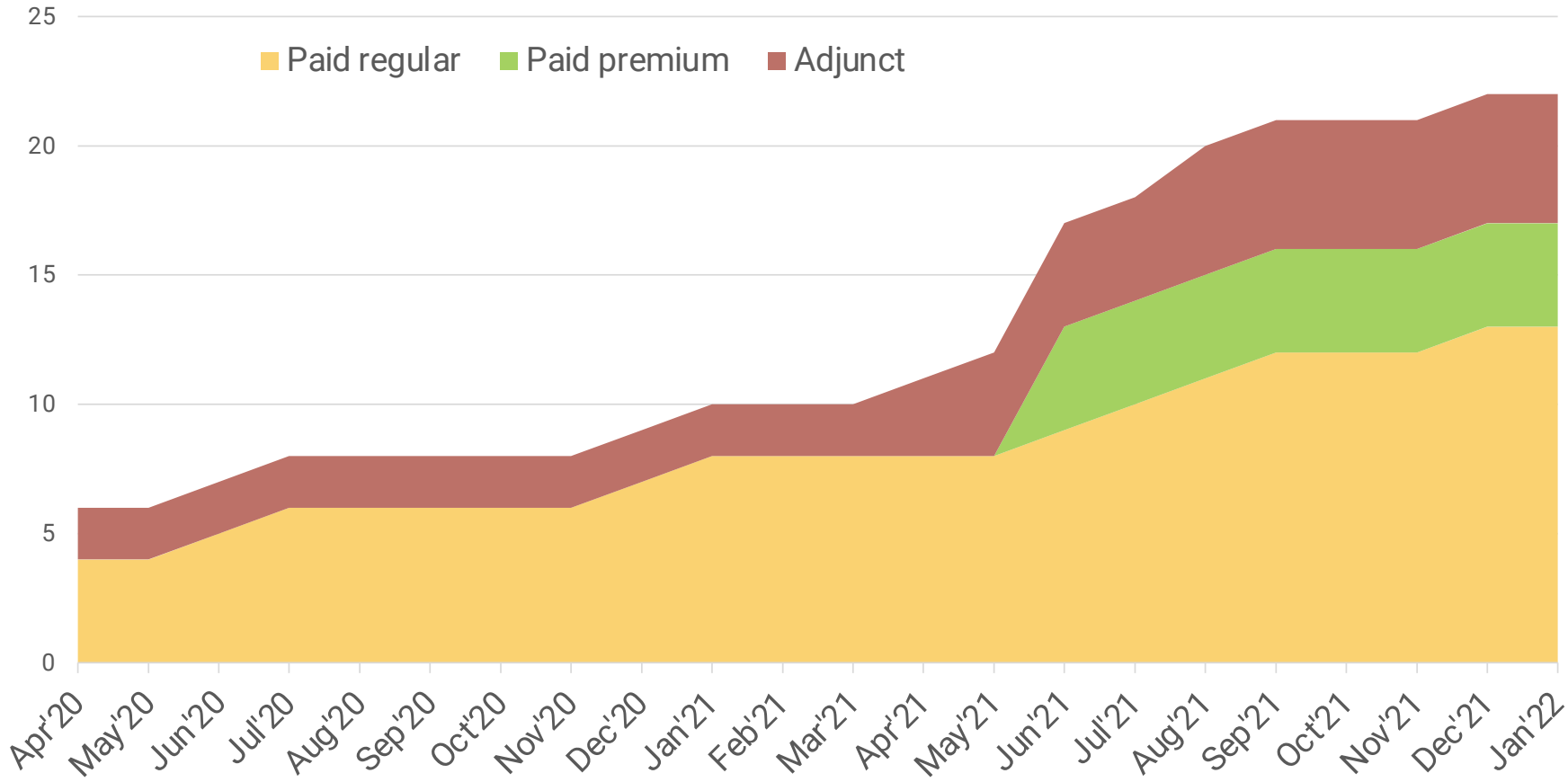


Brief seL4 History

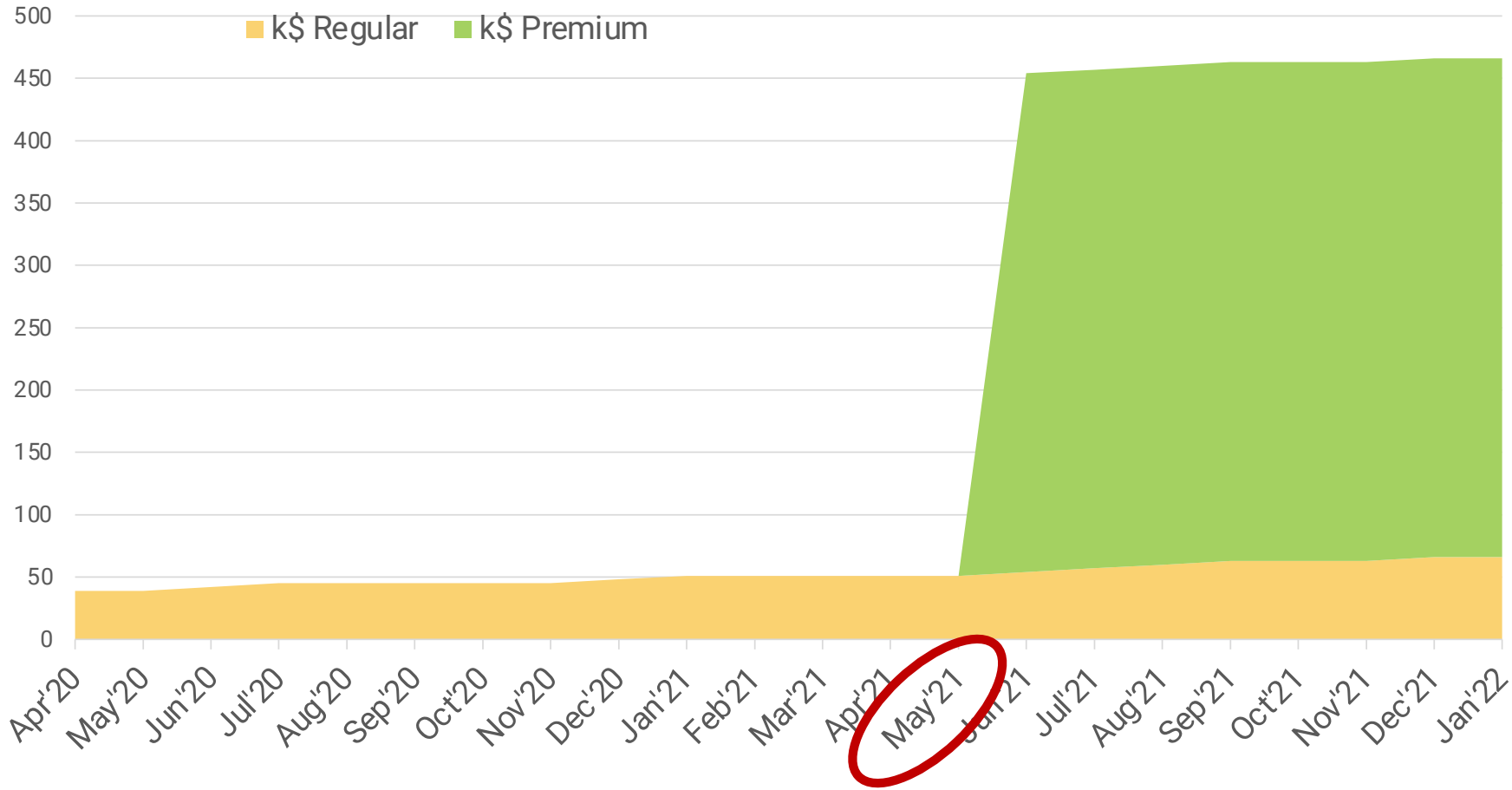
- 05–09: developed and implementation correctness proved at NICTA (Arm-32)
- 11–13: proofs of binary correctness, security enforcement, worst-case latencies
- Jul'14: open sourced (GPLv2)
- Jul'15: Boeing ULB helicopter flying autonomously on seL4
- Apr'17: DARPA HACMS final demos showing seL4 defeating 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

Foundation Membership



Foundation Budget



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

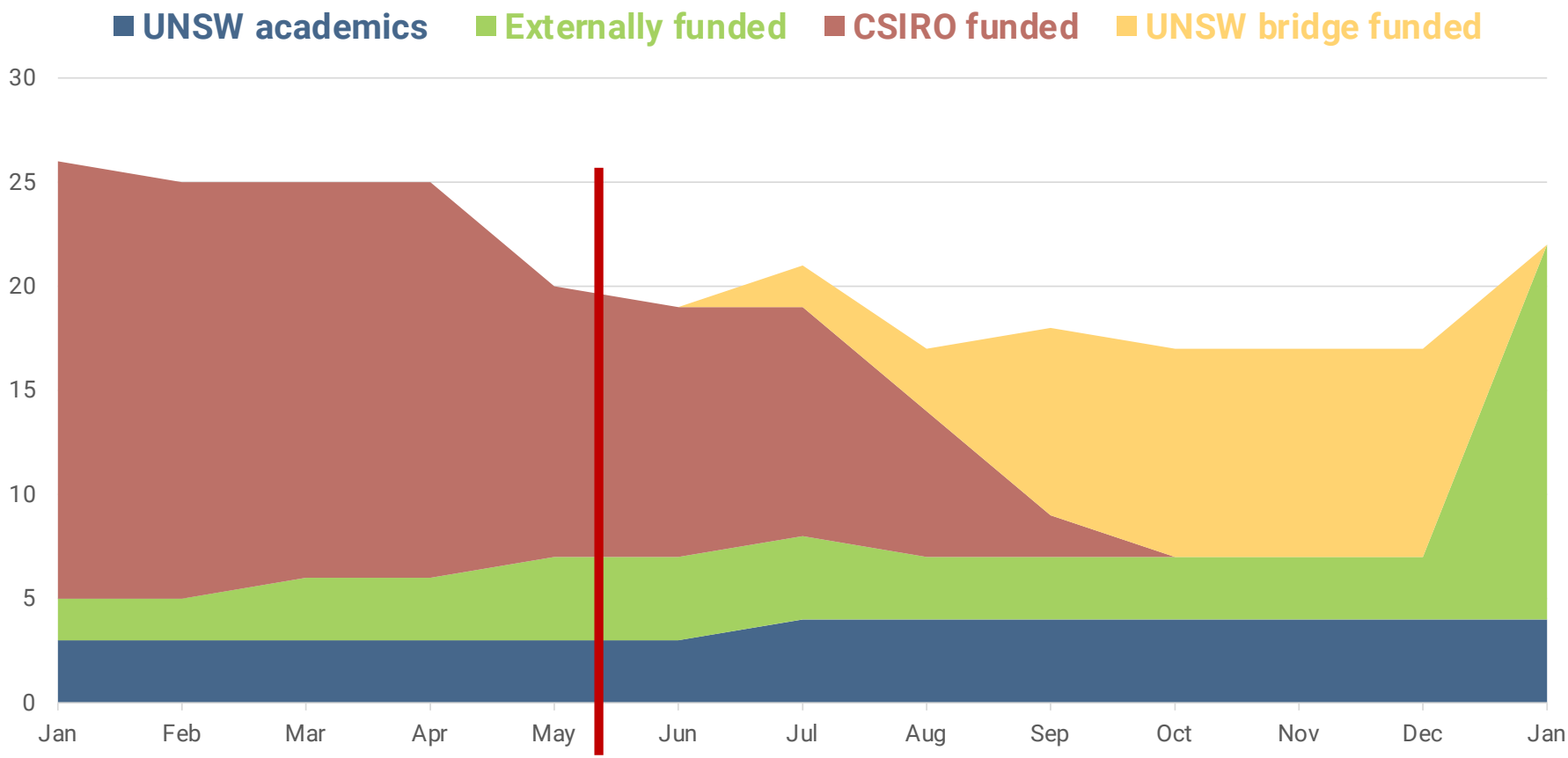
Joseph Brookes
Senior Reporter
31 May 2021

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.

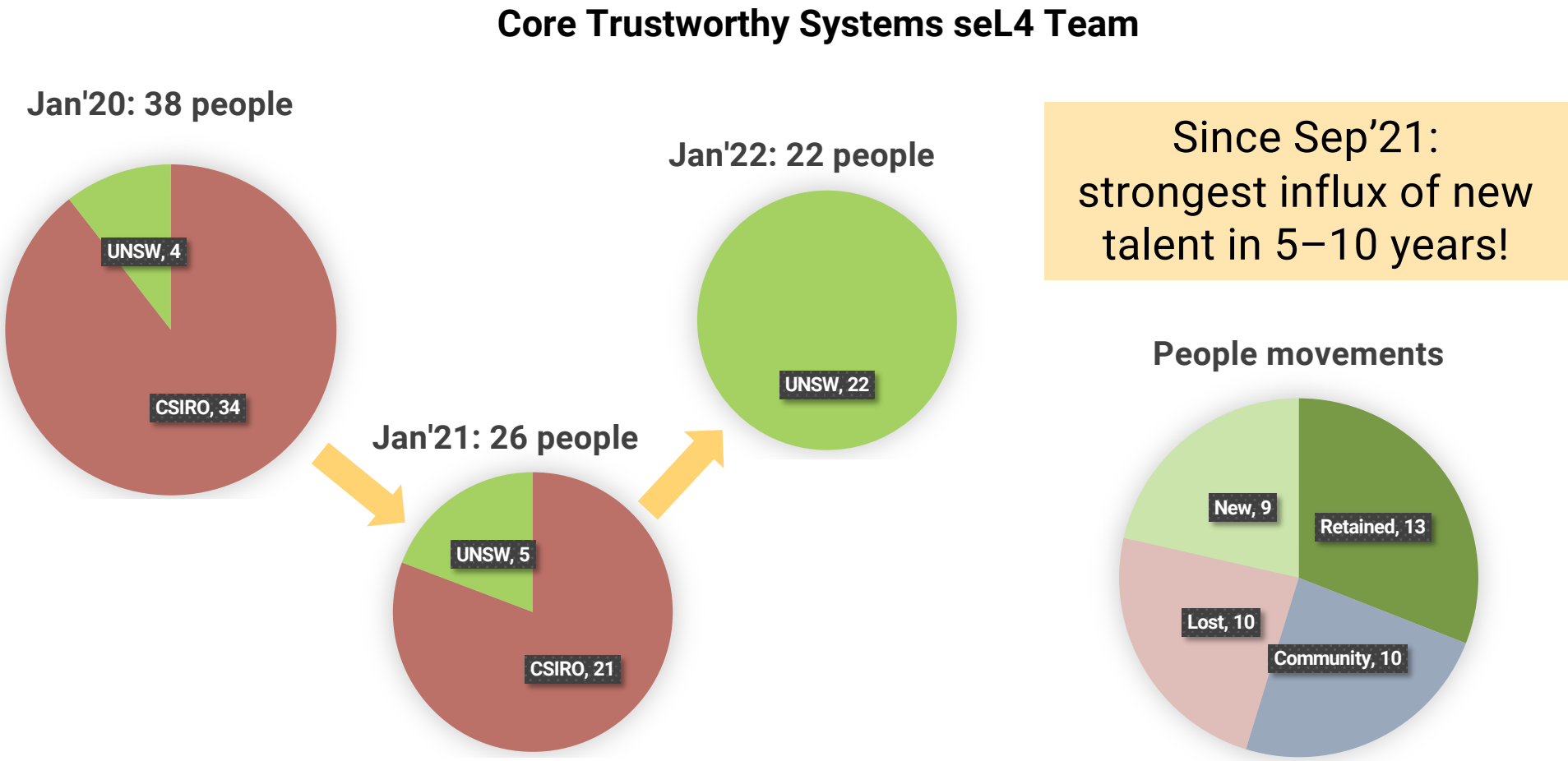
The new funding from UNSW School of Computer Science and Engineering will allow most of the Trustworthy Systems team – more than a dozen at the CSIRO and a

Life After CSIRO

On Life Support (UNSW Bridge Funding)



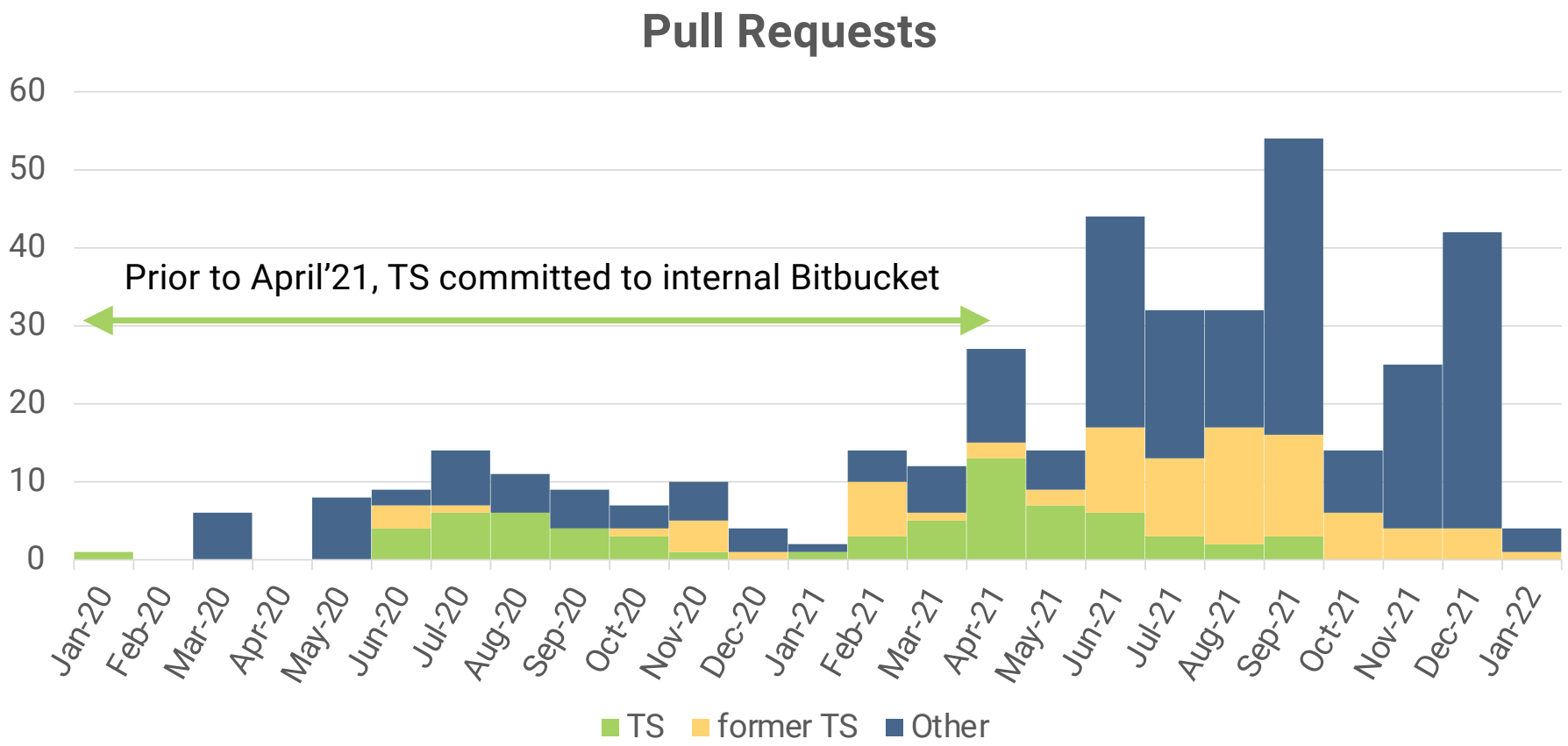
What Happened to TS People?



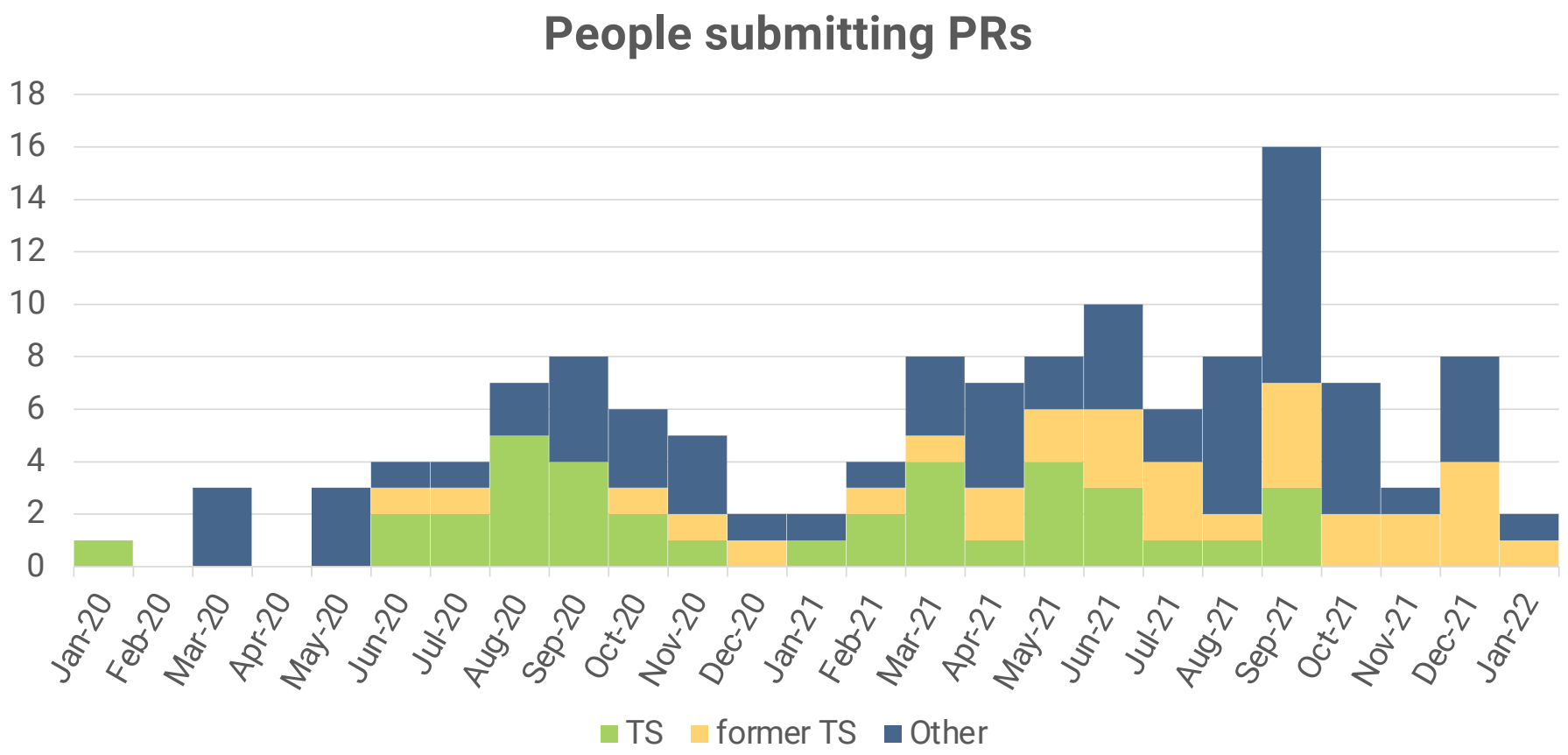
What's Behind This Development?

- 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



Community Growth



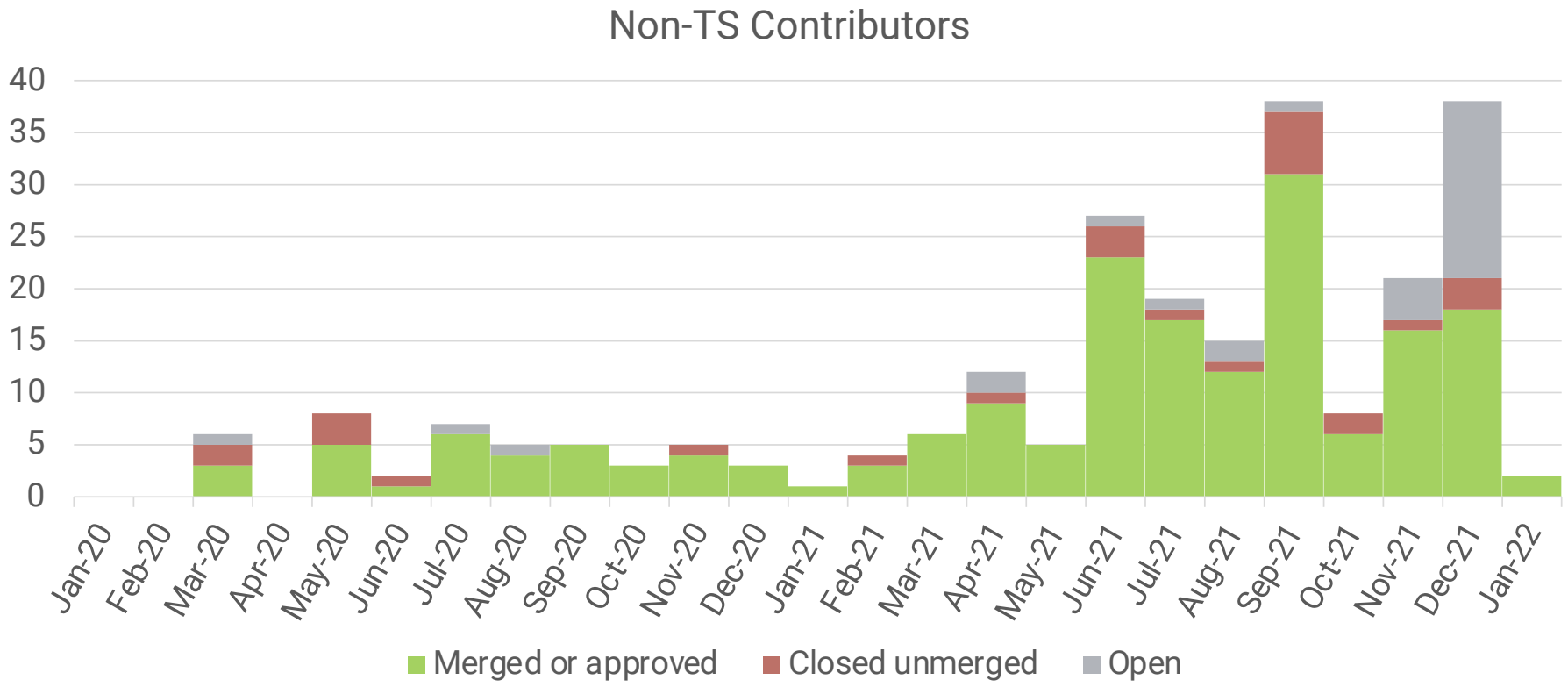
Why So Few PRs?

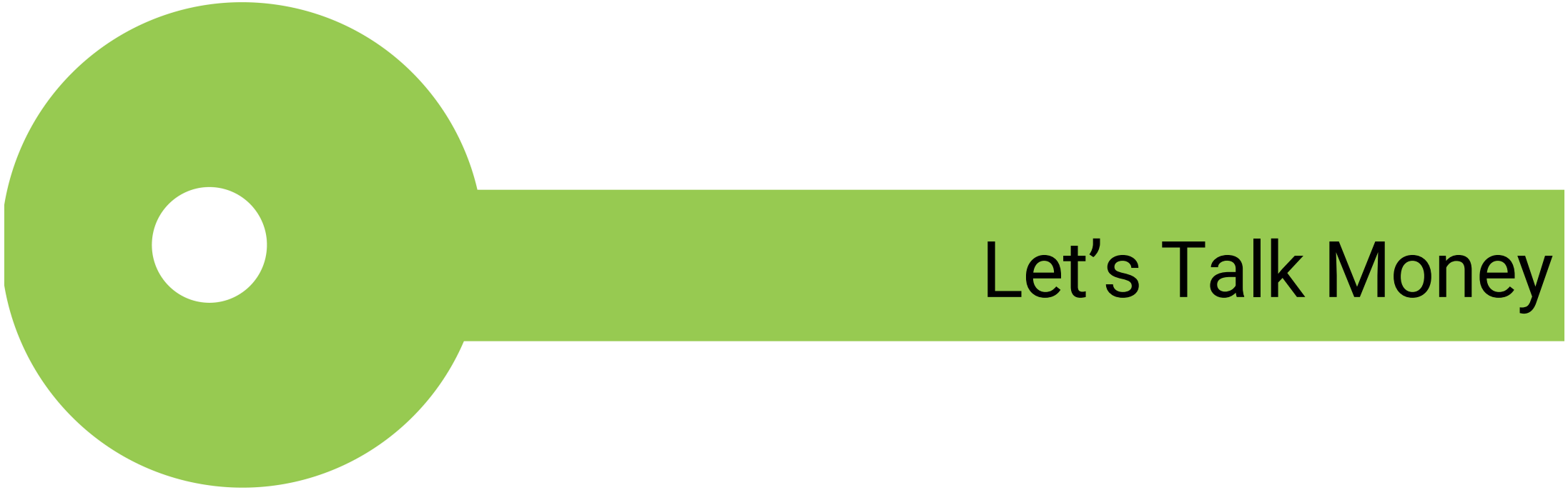
seL4 is a verified, high-performance microkernel!

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

Contributors must understand implications!

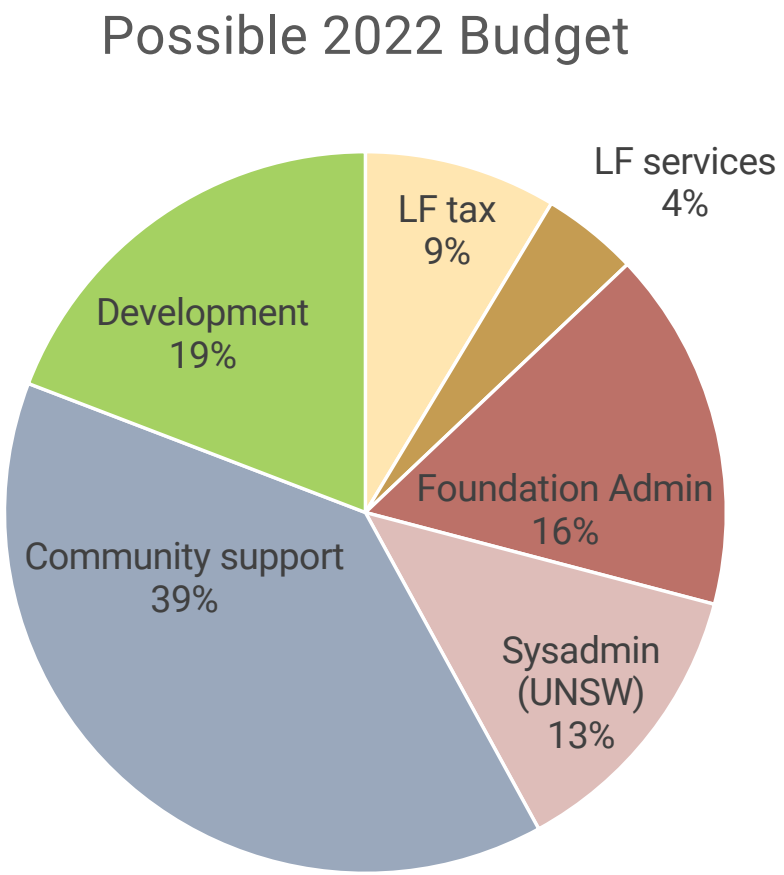
Success rates of “External” PRs



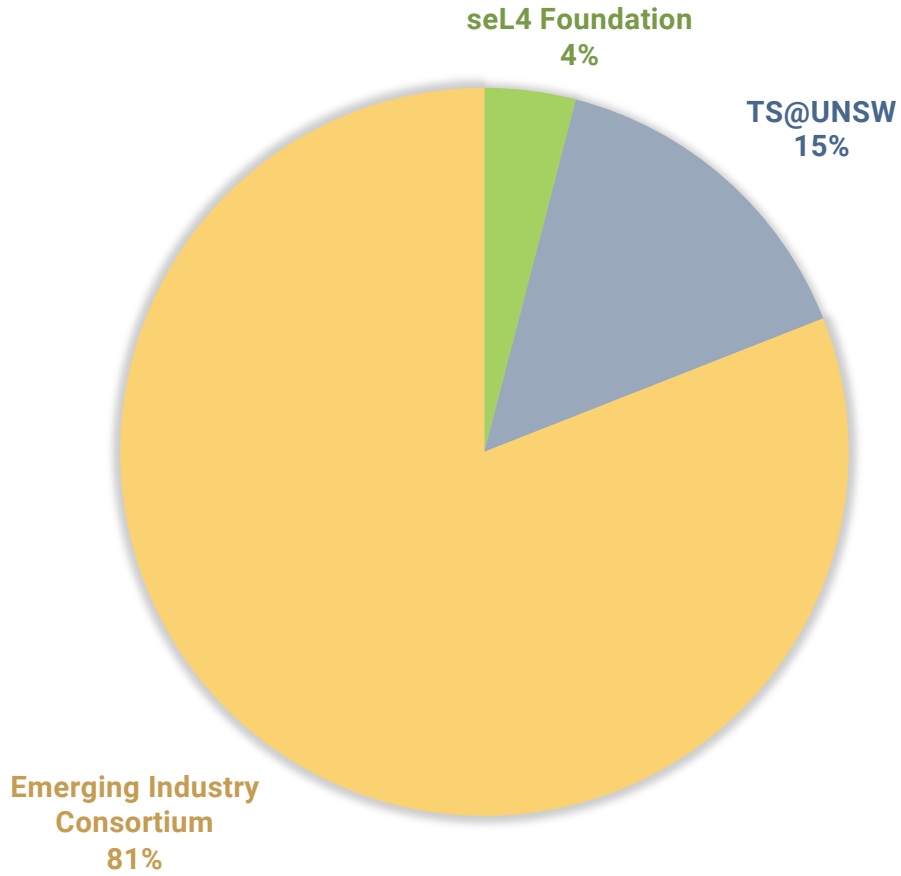


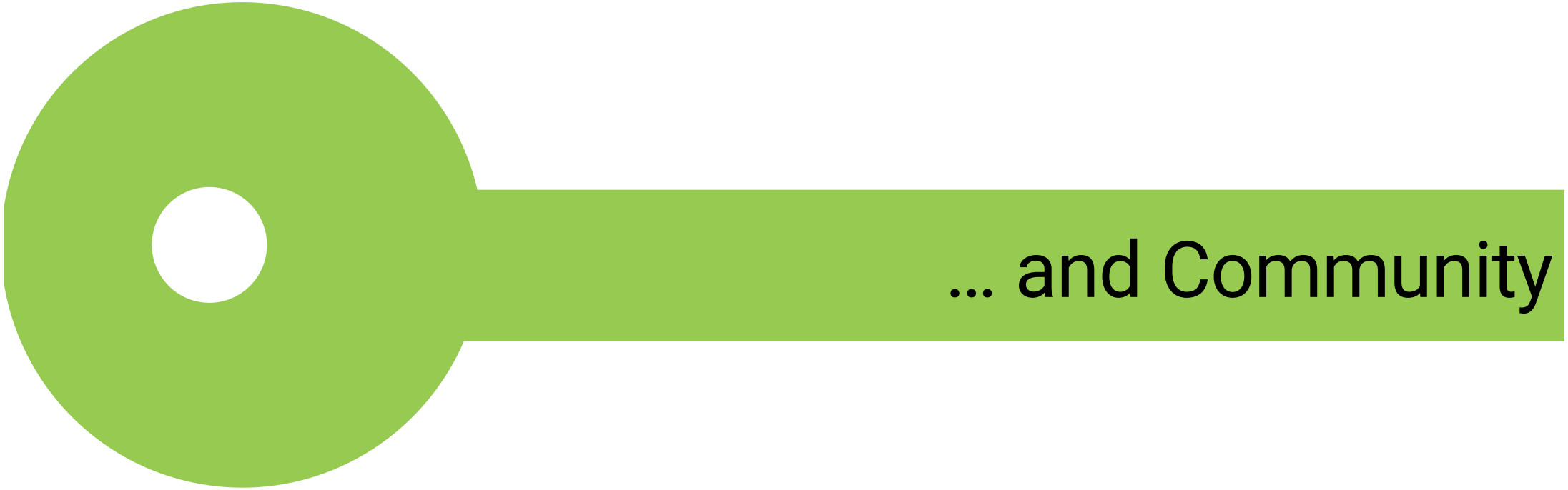
Let’s Talk Money

Putting Foundation $$ to Work



2022 Budgets in Comparison



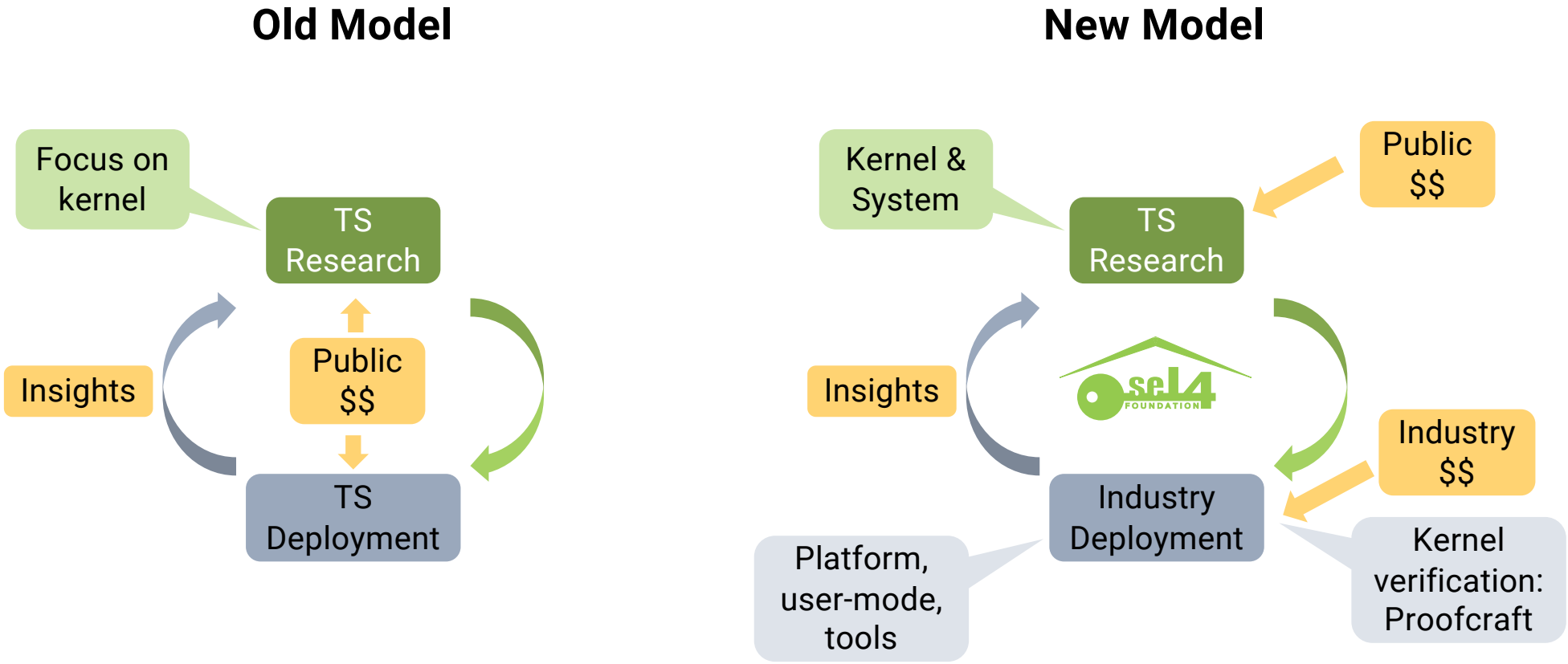


… and Community

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

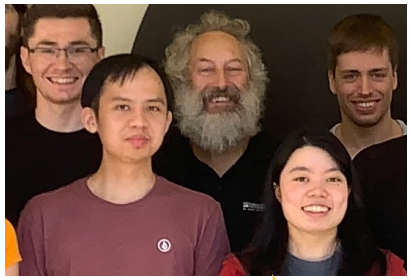
Implications: Development and Engagement



What’s Next for seL4?

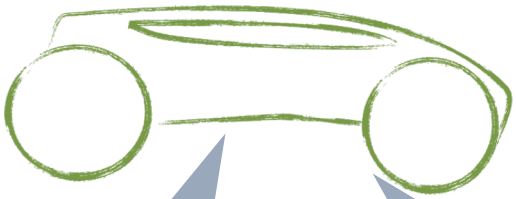
Community & Deployment Growth

Community development



Scaling up training

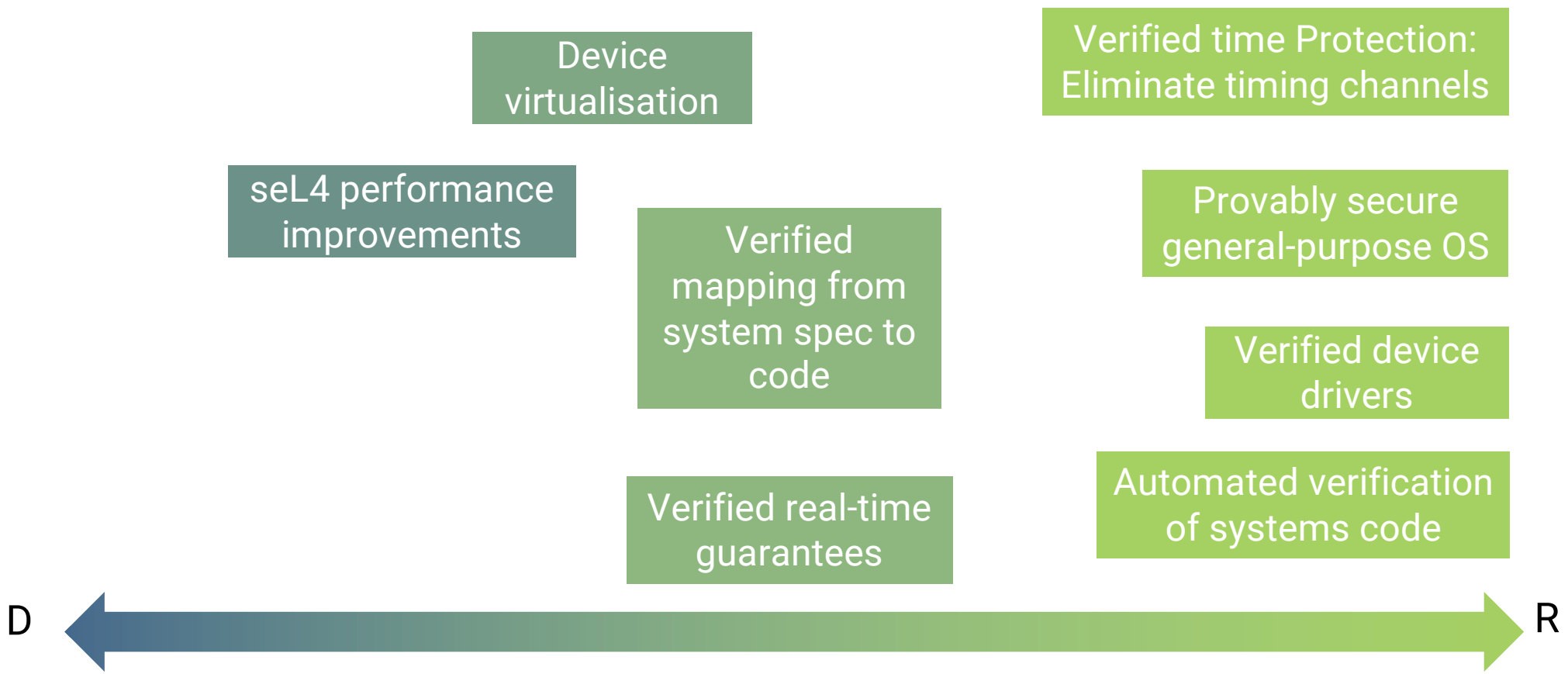
Entice ”lost” people back



Industry to develop secure car OS

Fund AArch64 & multicore verification

Research: Keep Redefining the State of the Art



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?