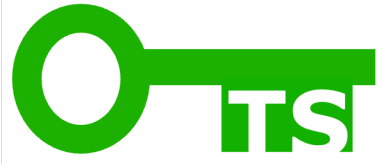
School of Computer Science & Engineering

Trustworthy Systems Group

Provable Security for Autonomous Vehicles

Gernot Heiser
UNSW Sydney and seL4 Foundation
gernot@unsw.edu.au



Car Hacking Danger Is Likely Closer Than You Think

A Detroit Free Press report shows there were 150 automotive cybersecurity incidents in 2019 alone.

BY SEBASTIAN BLANCO PUBLISHED: SEP 4, 2021

NATIONAL

Nearly 400 car crashes in 11 months involved automated tech, companies tell regulators

June 15, 2022 · 1:26 PM ET

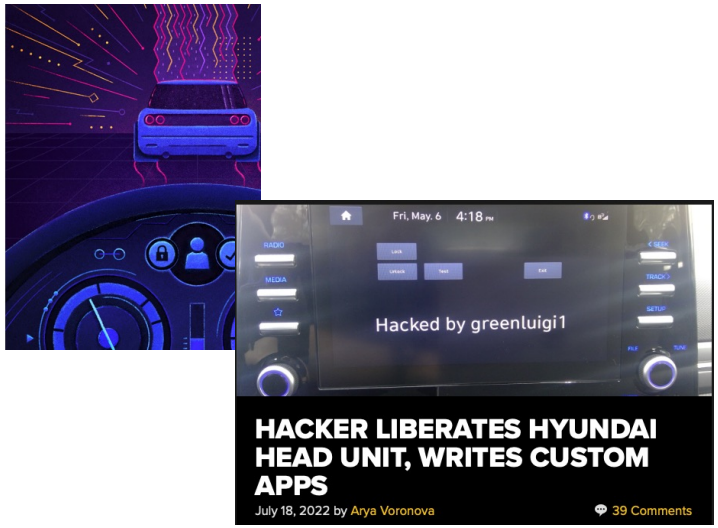
By The Associated Press

VULNERABILITIES

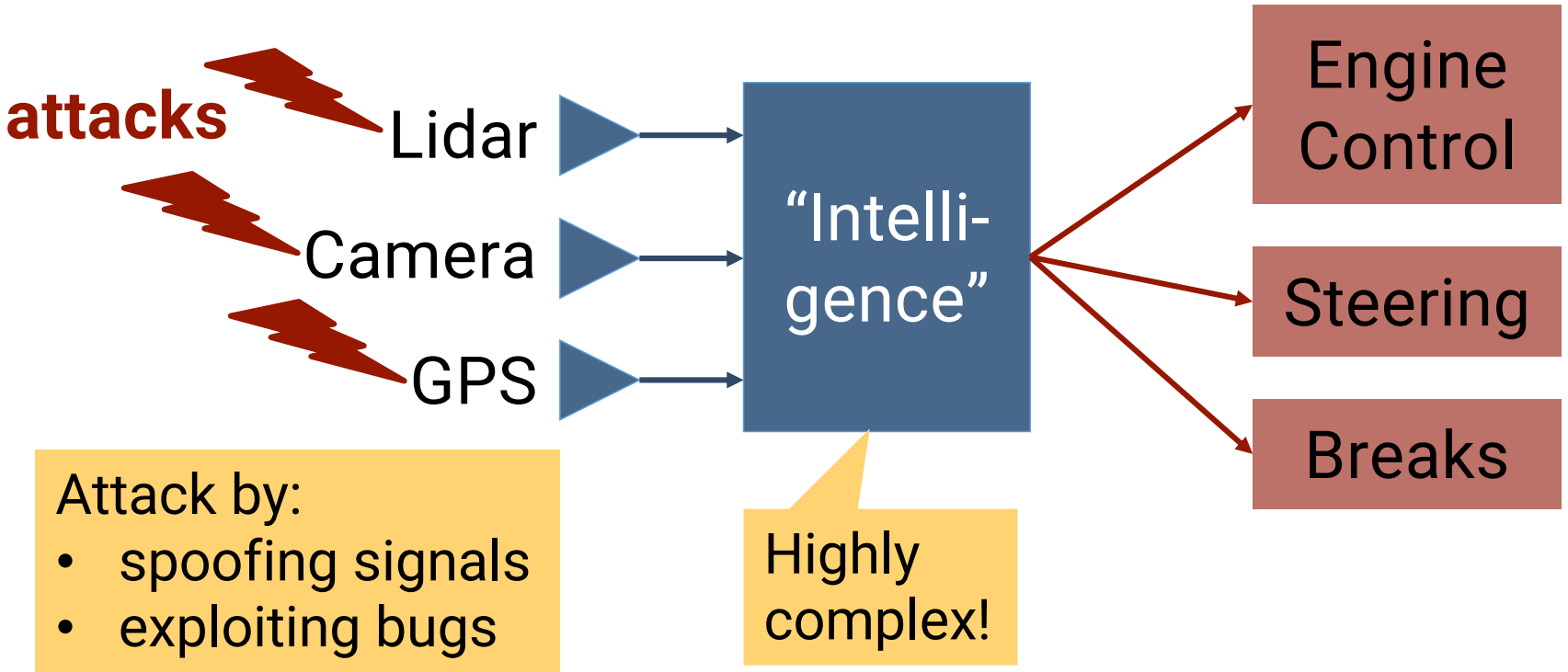
Car Hacking Is Real. Here's How Manufacturers Can Combat It

Sophisticated cars offer convenience for drivers but opportunities for hackers.

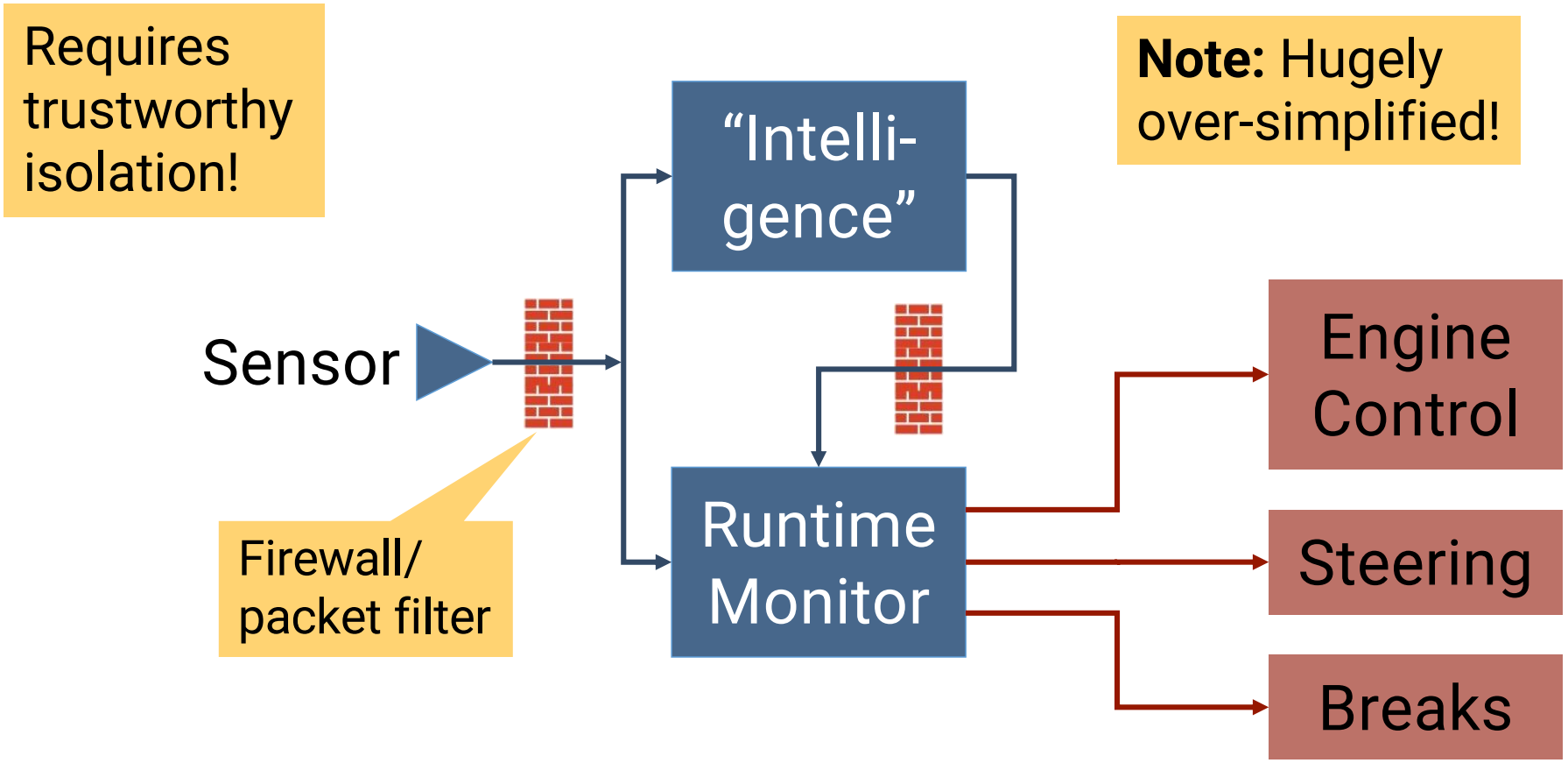
Diego Poza
Head of Content



Intelligent Vehicles: Hacker's Paradise!

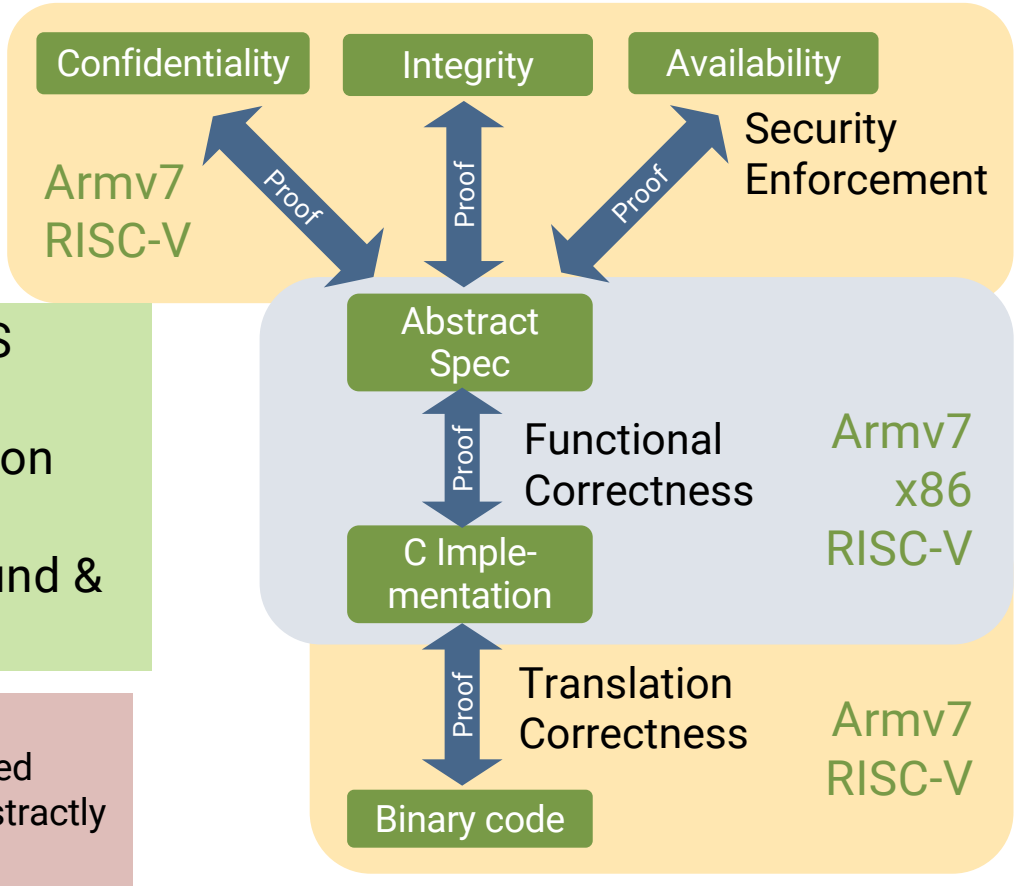


How Can We Protect Intelligent Vehicles?



Foundation for Truly Secure Systems

AArch64 in progress

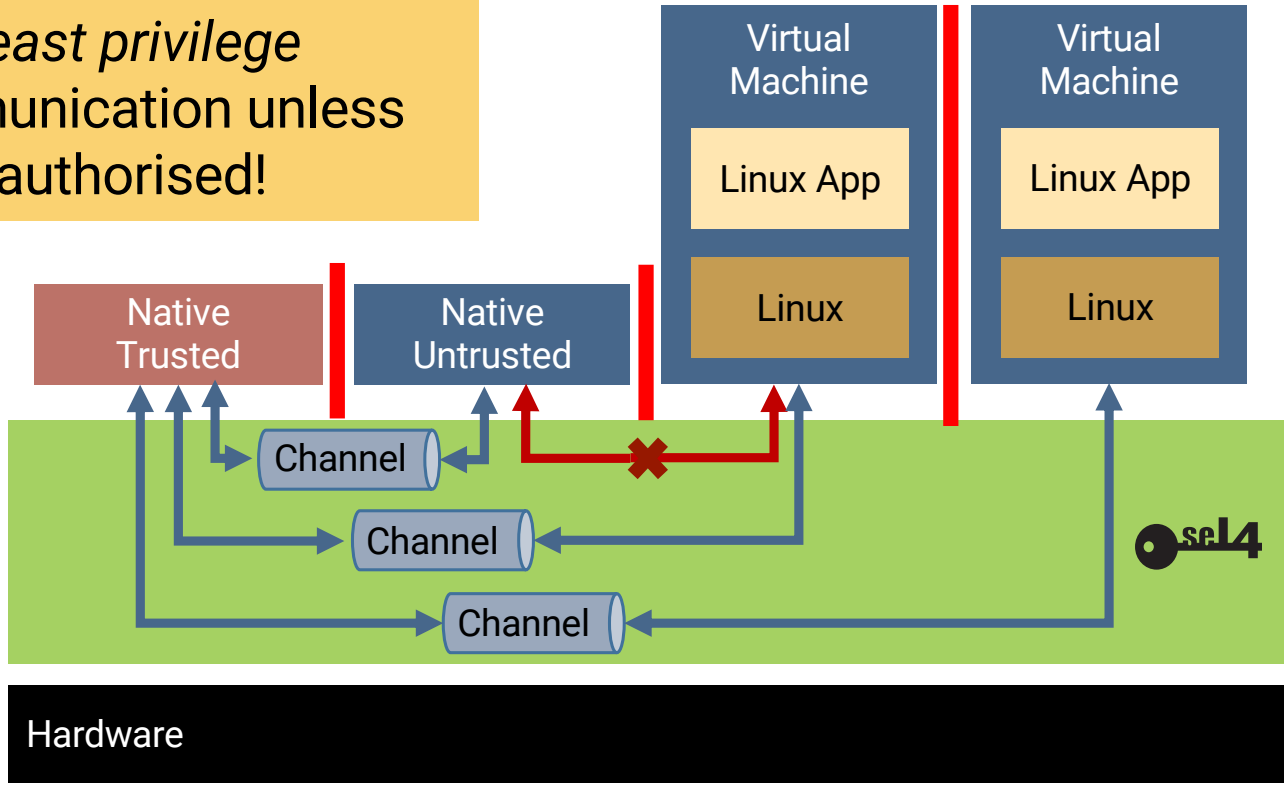


- World's first correctness proof of OS
- Comprehensive formal verification
- Capabilities for fine-grained protection
- World's fastest microkernel
- Only protected-mode RTOS with sound & complete WCET analysis (Armv6)

Present limitations
- initialisation code not verified
- MMU, caches modelled abstractly
- Multicore not yet verified

Capabilities: Fine-Grained Protection

- Enforce *least privilege*
- No communication unless explicitly authorised!



The Benchmark for Performance

Smaller is better

World's fastest microkernel!

Round-trip cross-address-space IPC on 64-bit Intel Skylake

	seL4	Fiasco.OC L4Re	Zircon
Latency (cycles)	986	2717	8157
Mandatory HW cost* (cycles)	790	790	790
Overhead absolute (cycles)	196	1972	7367
Overhead relative	25%	240%	930%

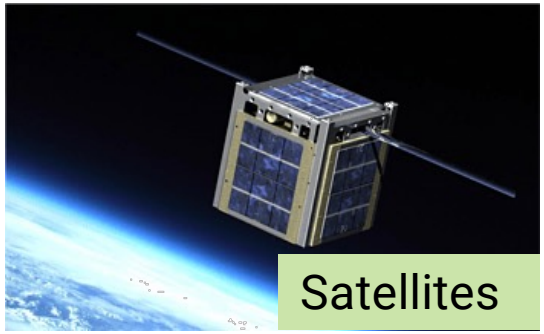
*: The Cost of `SYCALL` + 2 × `SWAPGS` + `SYSRET` = 395 cycles, times 2 for round-trip

Source:

Zeyu Mi, Dingji Li, Zihan Yang, Xinran Wang, Haibo Chen: "SkyBridge: Fast and Secure Inter-Process Communication for Microkernels", EuroSys, April 2019

Made For Real-World Use

Autonomous vehicles



Satellites

Secure communication device
In use in multuiple defence forces

Laot: Critical infrastructure protection

DARPA: World's Most Secure Drone

← Tweet

DARPA @DARPA

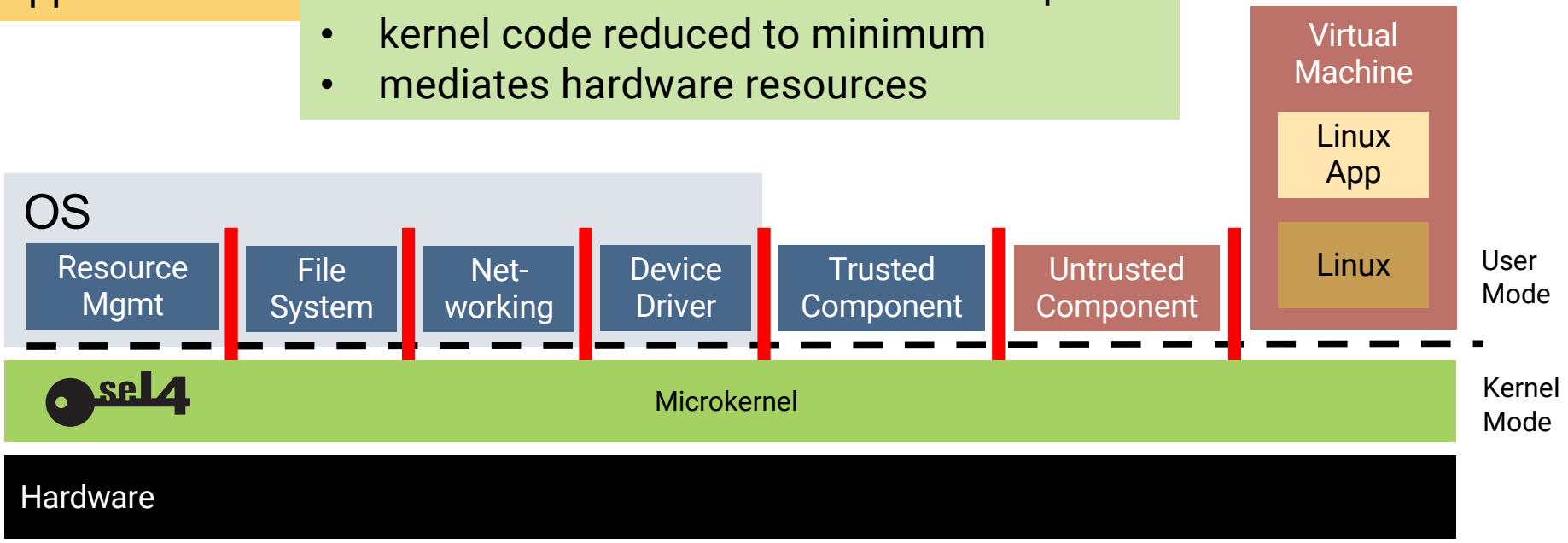
We brought a hackable quadcopter with defenses built on our HACMS program to @defcon #AerospaceVillage. As program manager @raymondrichards reports, many attempts to breakthrough were made but none were successful. Formal methods FTW!

seL4-based OS

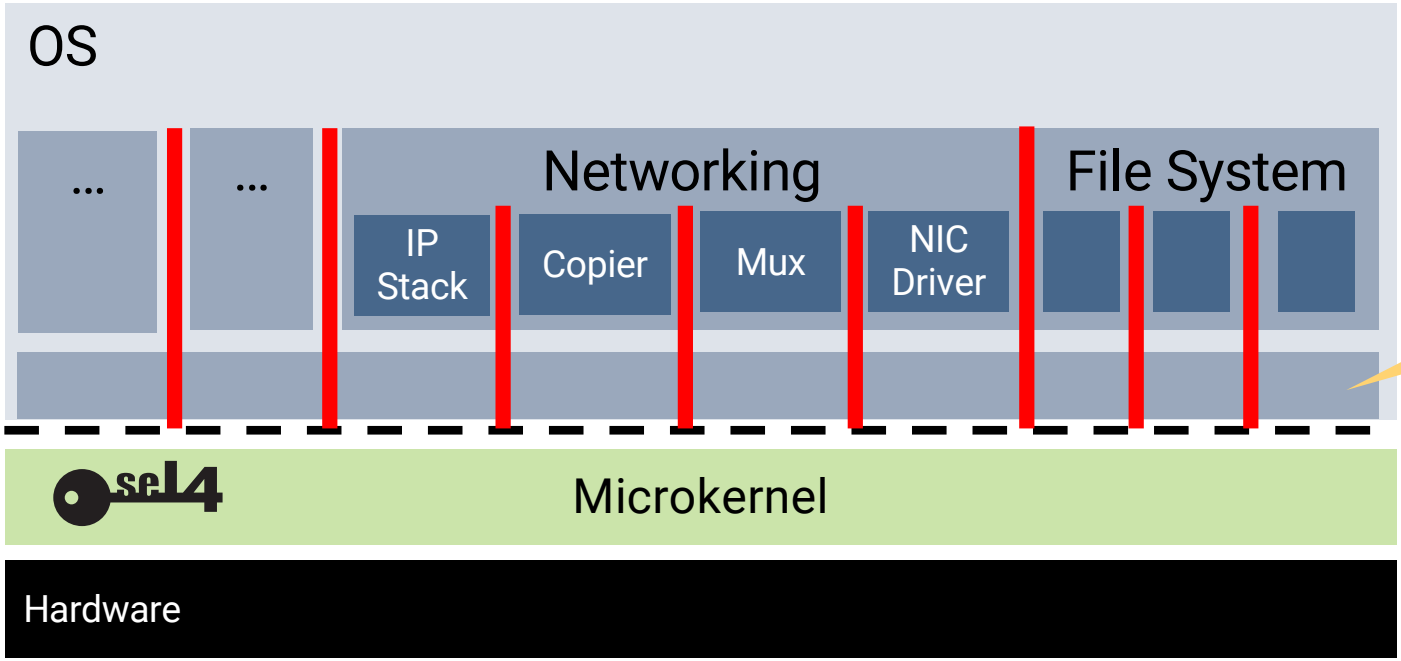
Microkernel Is Not An OS

Modularisation: Separate components
- operating-system services
- device drivers
- applications

Microkernel enforces isolation – bullet-proof
- kernel code reduced to minimum
- mediates hardware resources



A Modular seL4 OS



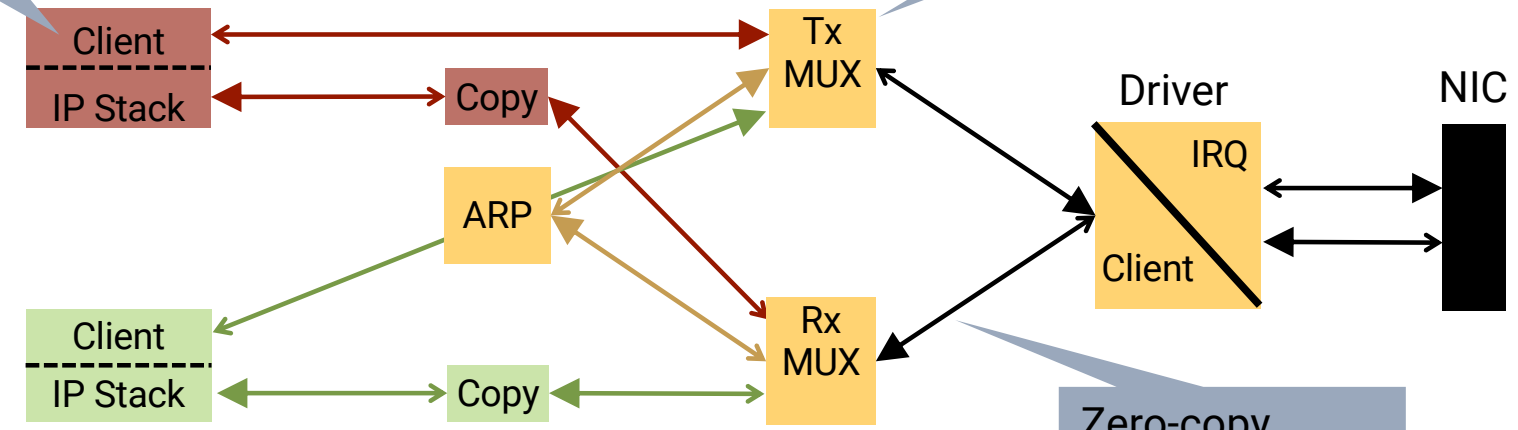
seL4 Core Platform:
Thin abstraction layer

Example: Networking

- Async I/O interface
- Optional Posix-like front-end

Strict separation of concerns: Large number of extremely simple components

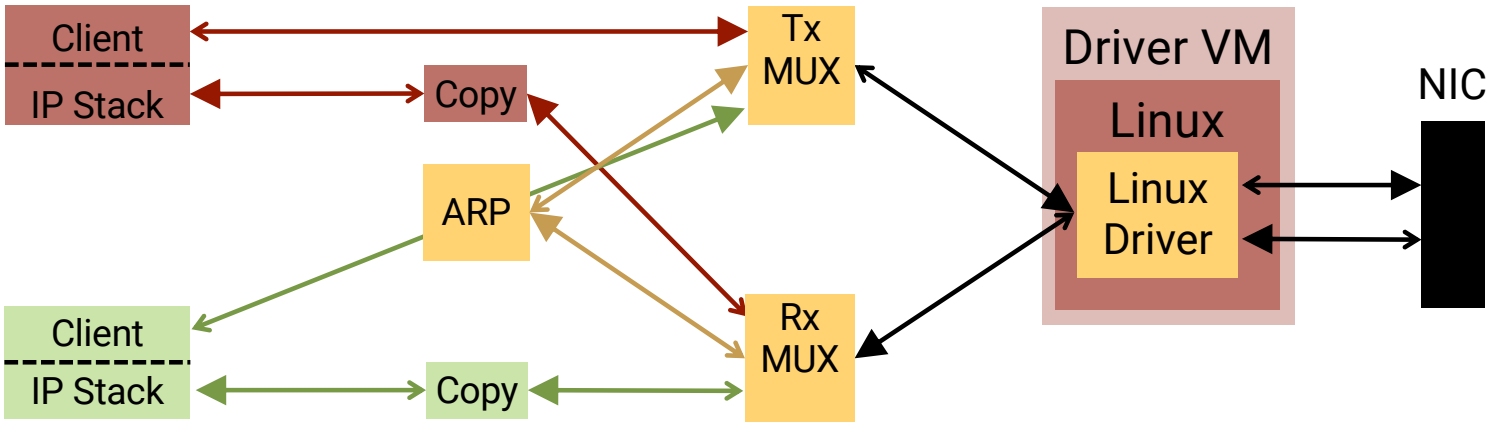
Multiplexer for device sharing and traffic shaping



Zero-copy shared-memory communication

Legacy Drivers?

Can use Linux drivers wrapped into individual driver VM



Comparison to Linux

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

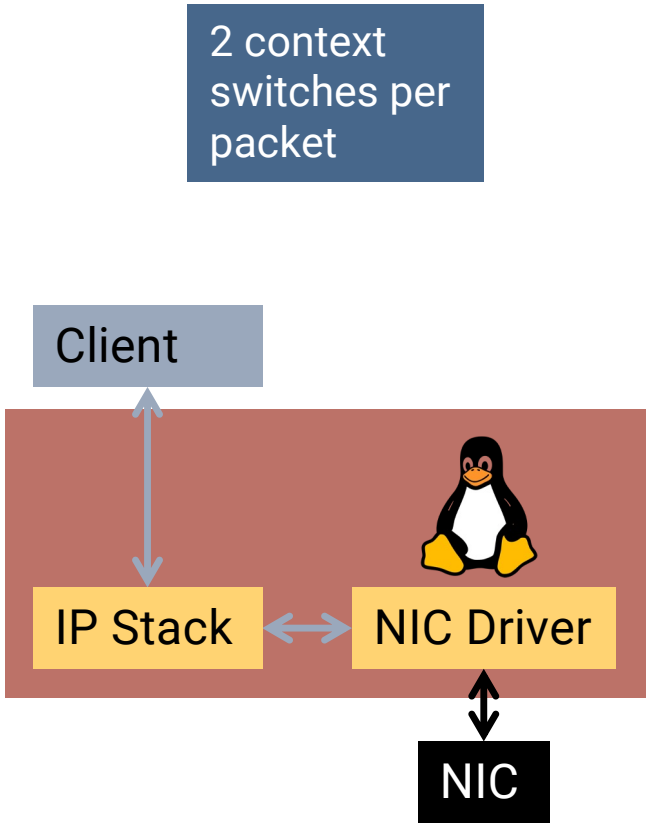
Performance?

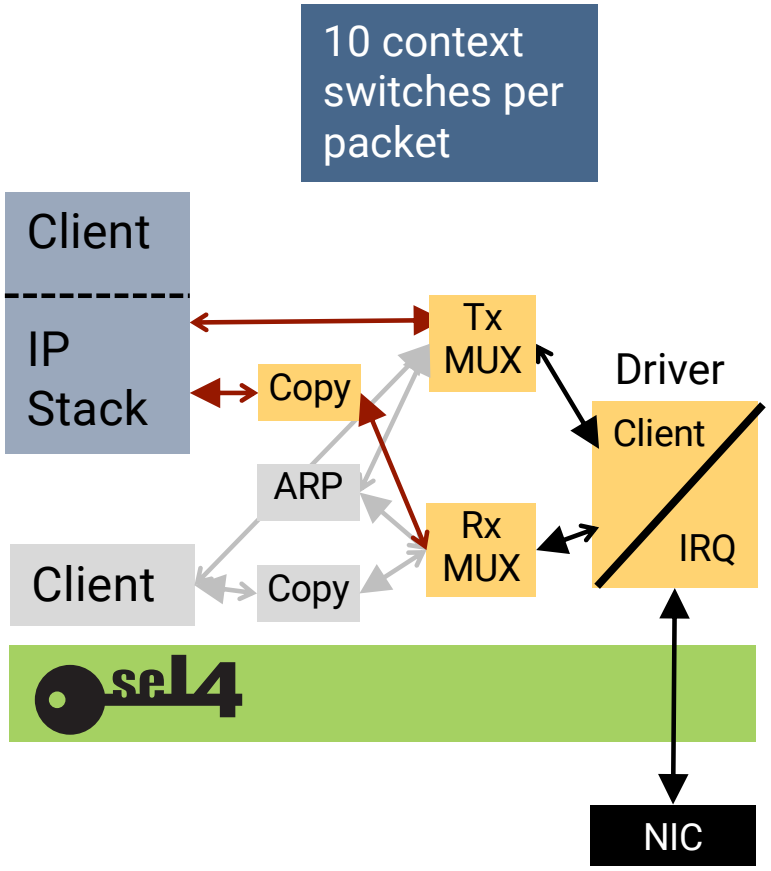
Written by second-year student!

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 enough to apply push-button verification!

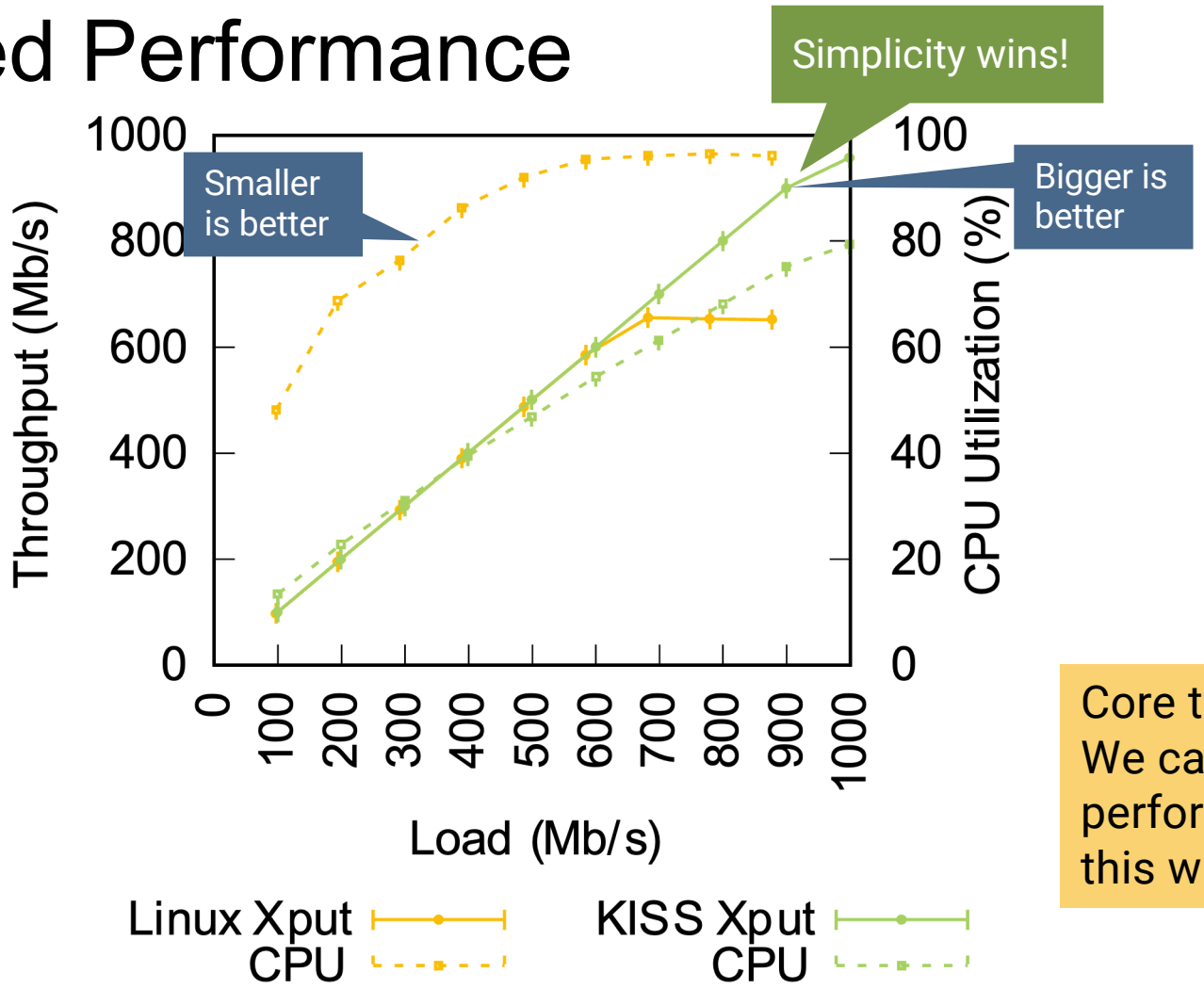
Evaluation Setup





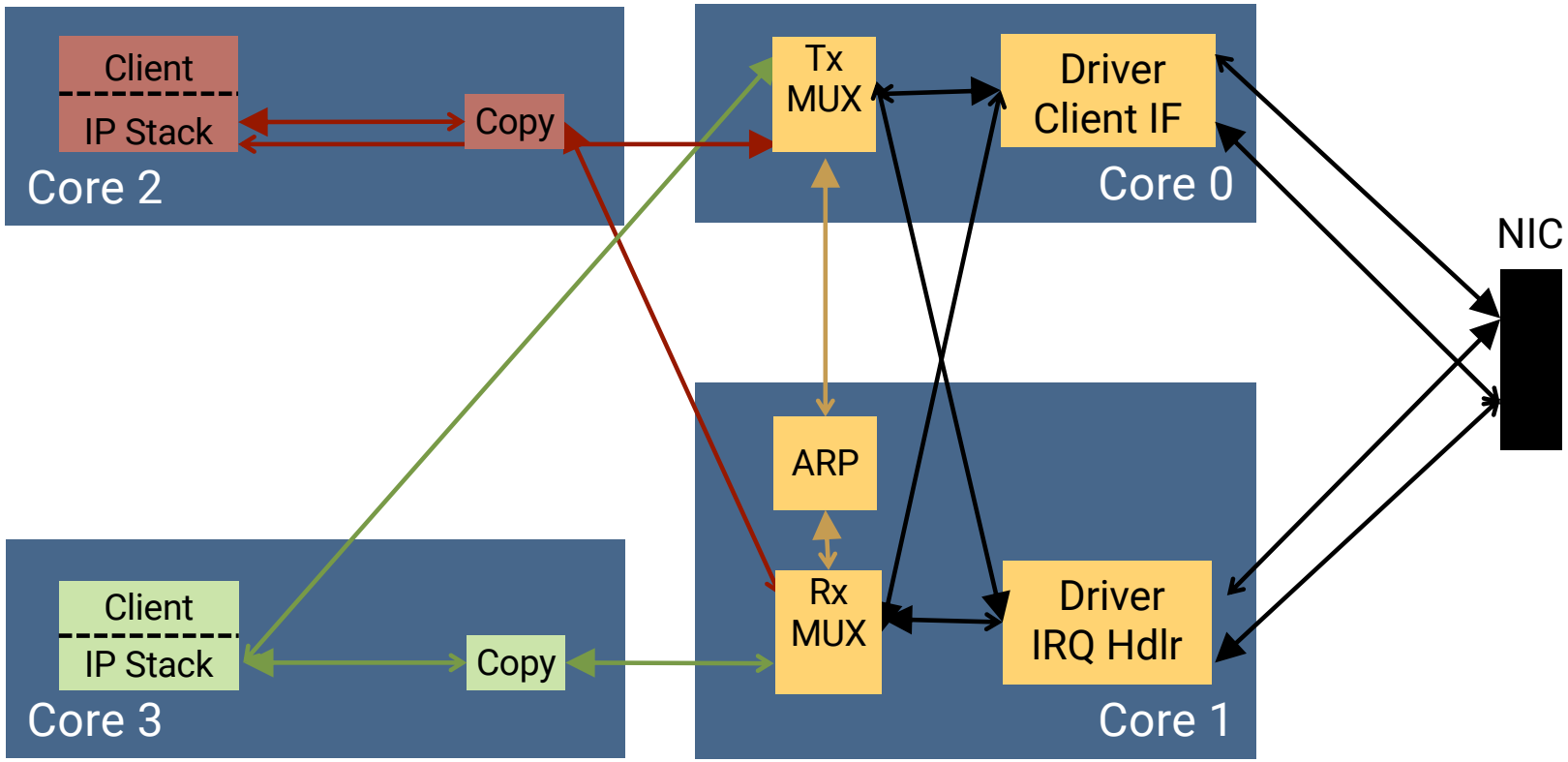
Achieved Performance

- Gigabit Ethernet
- single core

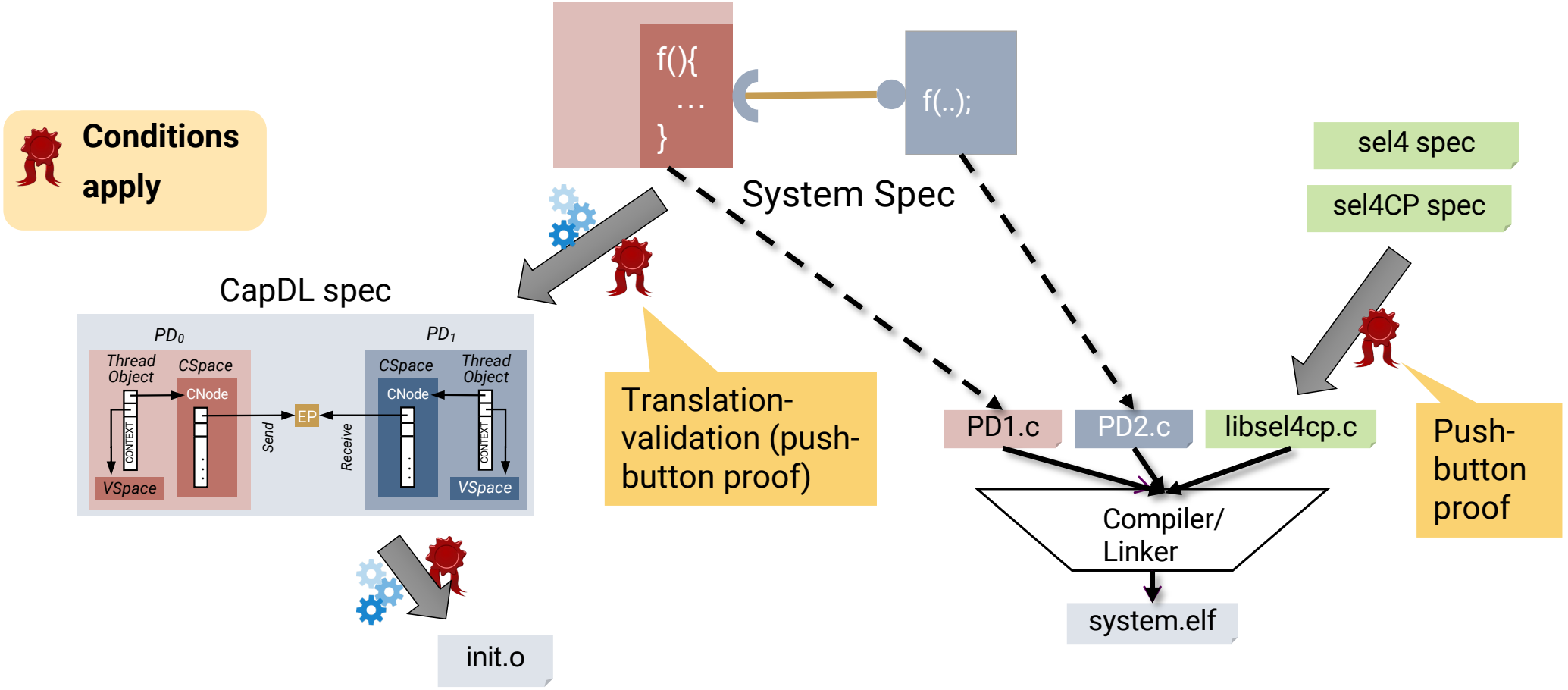


Core take-away: We can build a performant OS this way!

Multicore Example

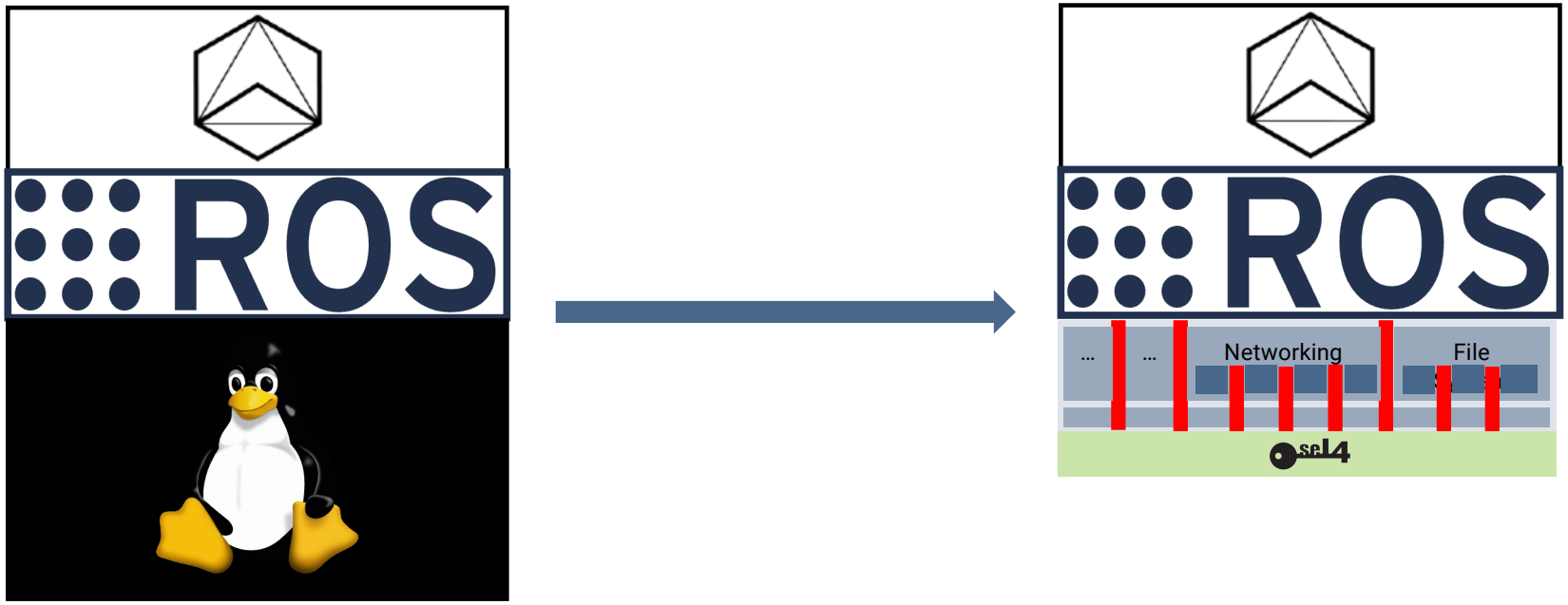


OS Verification



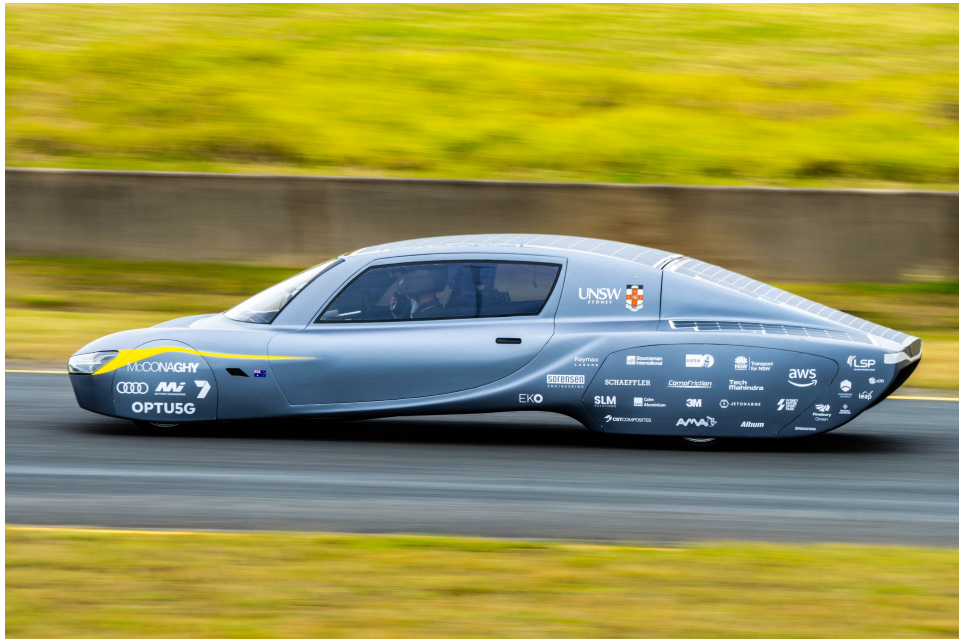
seL4 and Autoware

Autoware on seL4?



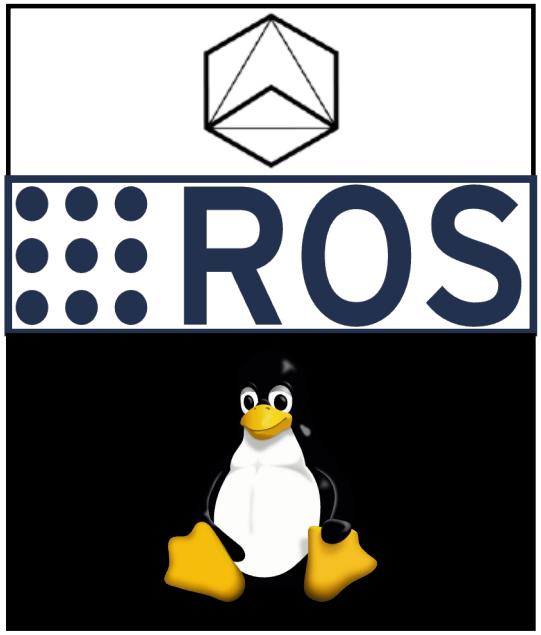
Porting ROS 2: Initial Experience

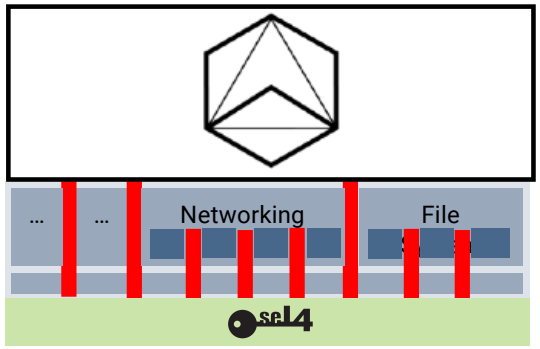
- Current driver is UNSW's Sunswift Solar Racing Car
- In theory, ROS 2 has an OS abstraction layer:
  - ROS 2 Core Utilities
  - ROS 2 Runtime C
- In practice, ROS 2 implementation basically assumes Linux underneath
  - need to analyse more how a port could really work
  - stay tuned…



Autoware on seL4 – Alternative Approach

To be investigated!





Security is no excuse for bad performance!

https://trustworthy.systems