Security Is No Excuse for Poor Performance!

Welcome to the world's most highly assured operating system

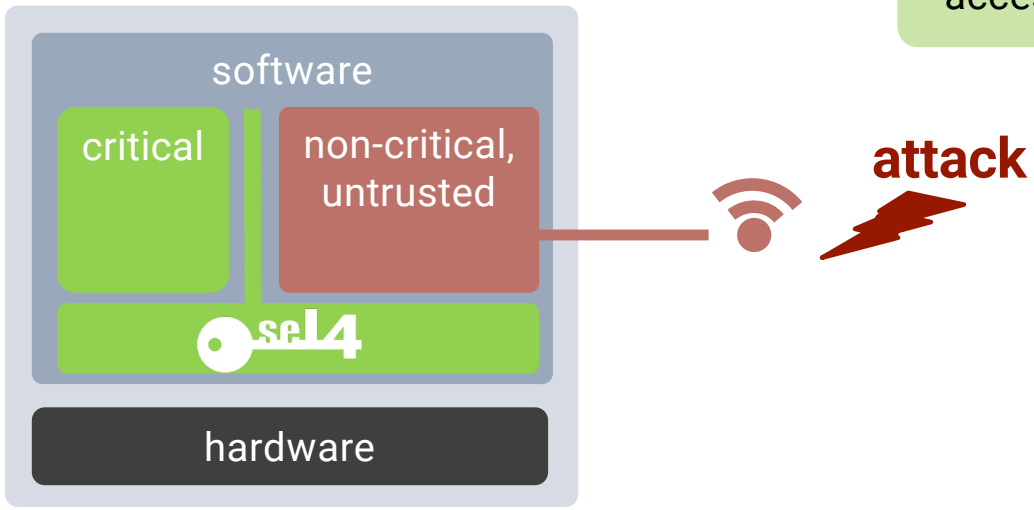
Gernot Heiser
Chairman, seL4 Foundation
Trustworthy Systems @ UNSW Sydney

gernot@sel4.systems

What is seL4?

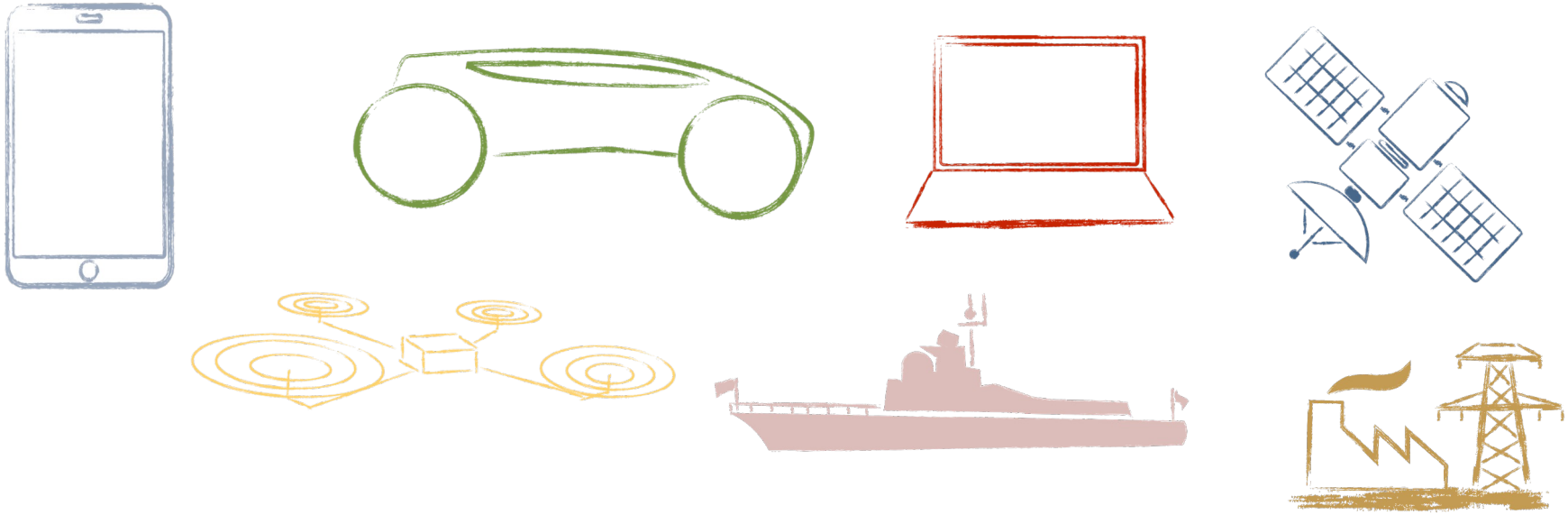
seL4 is an open source, high-assurance, high-performance operating system microkernel

- 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

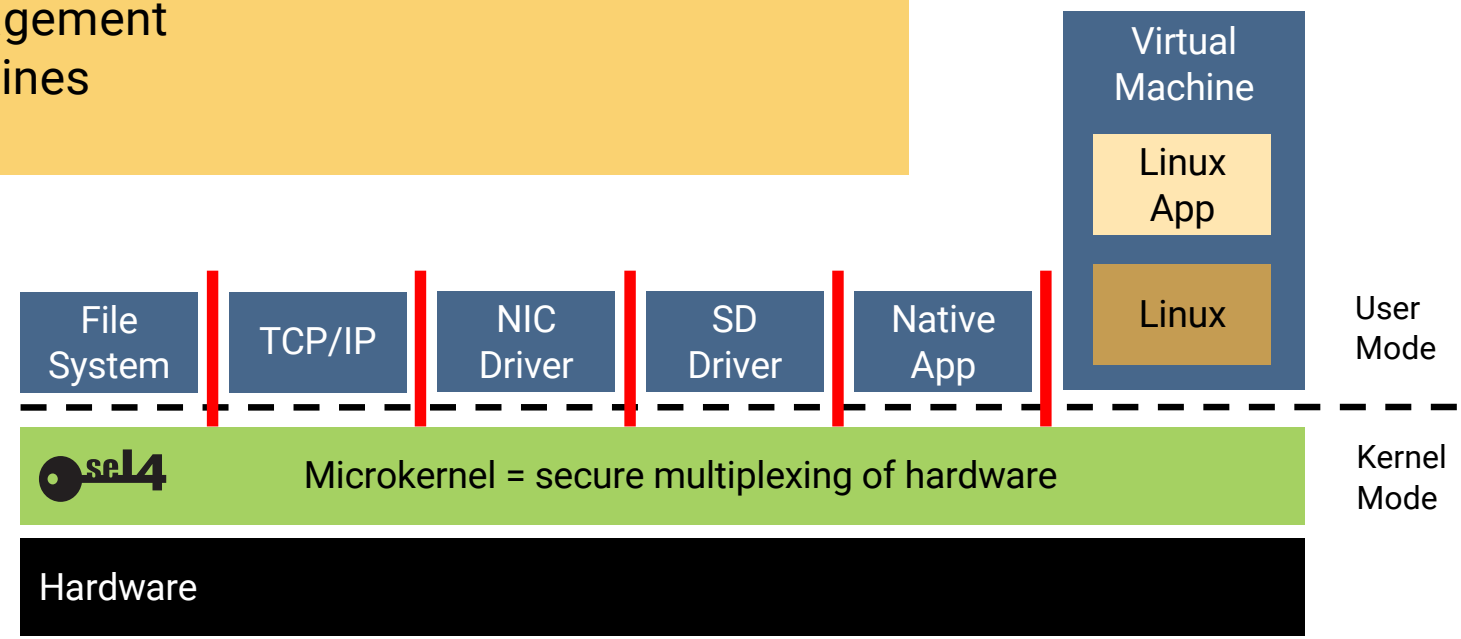


Already in use across many domains:
automotive, aviation, space, defence, critical infrastructure, cyber-physical systems, IoT, industry 4.0, certified security...

A Microkernel is not an Operating System

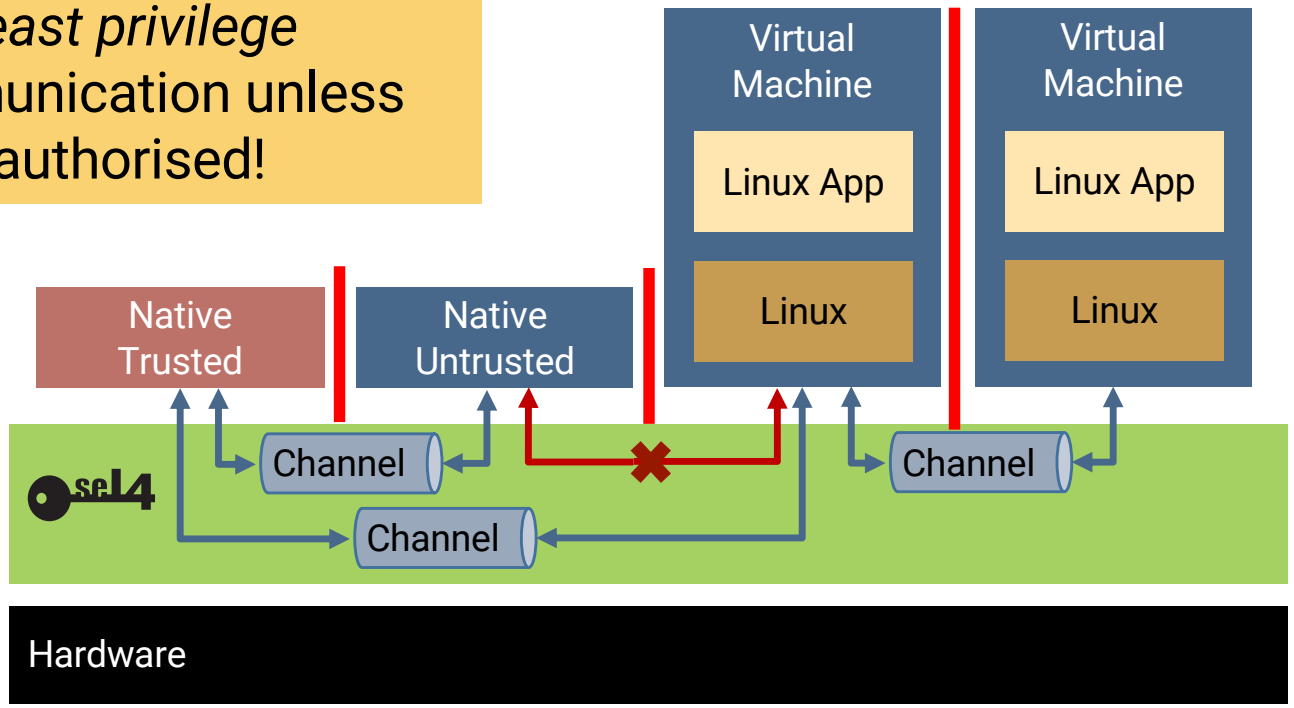
All operating-system services are user-level processes:

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



“Capabilities”: Controlled Communication

- Fine-grained access control
- Enforce *least privilege*
- No communication unless explicitly authorised!



The Benchmark for Performance

Latency (in cycles, **small is good**) of a round-trip, cross-address-space IPC on x64

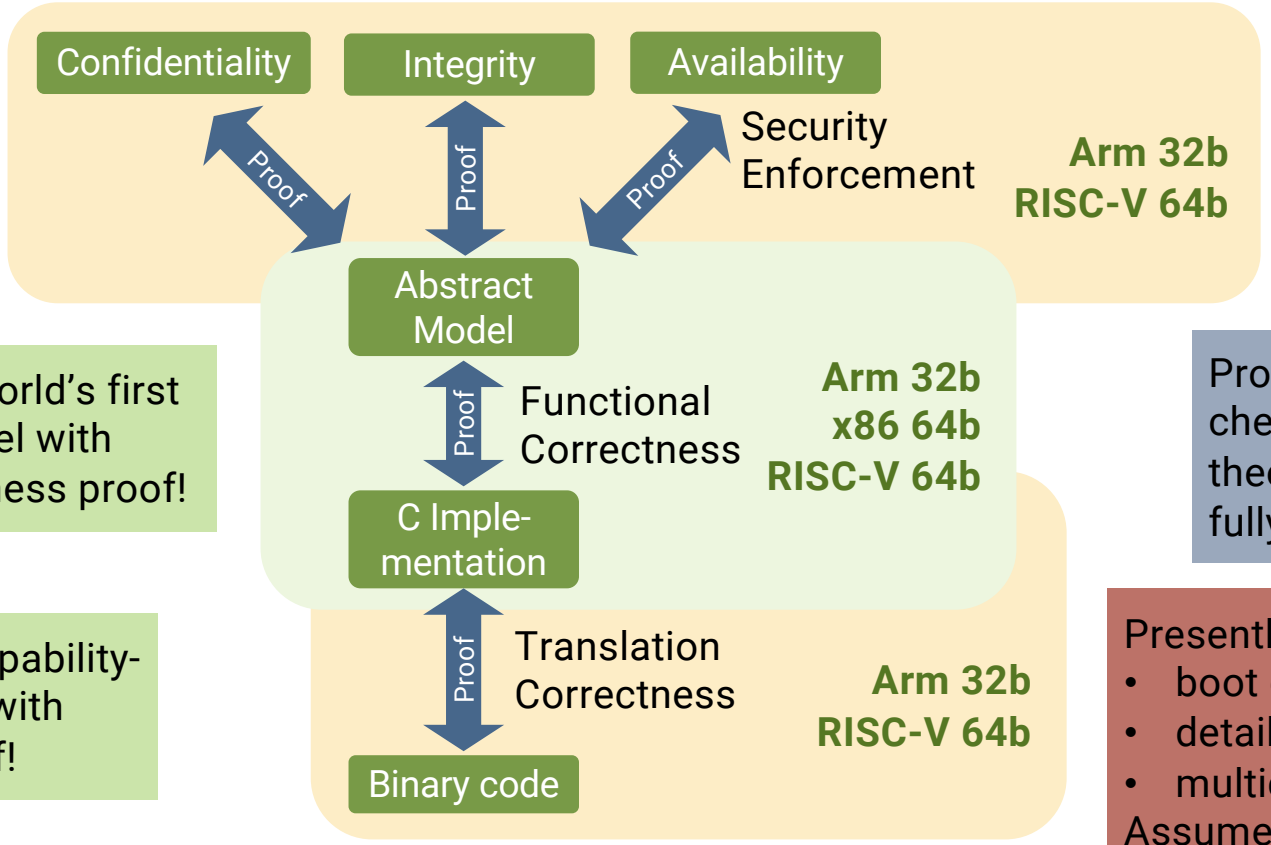
World's fastest microkernel!

Source	**seL4**	Fiasco.OC	Zircon
Mi et al, 2019	**986**	2717	8157
Gu et al, 2020	**1450**	3057	8151
seL4.systems, May'22	**760**	– –	– –

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 2022-05-07

Unique Verification by Mathematical Proof



Arm 64b
in progress
(thanks NCSC!)

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

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

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

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

Assume HW operates correctly

What Does This Mean?

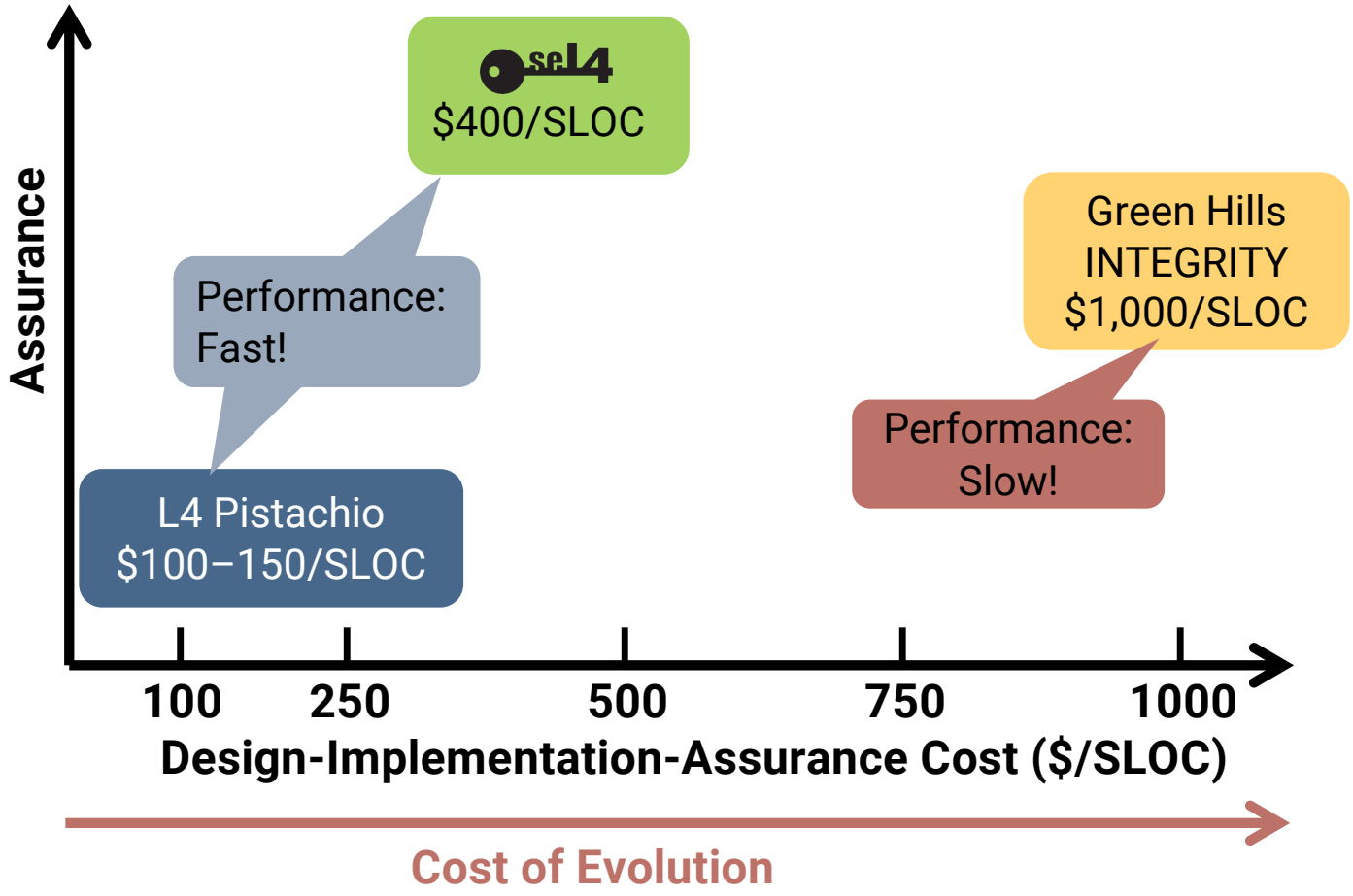
Kinds of properties proved for functional correctness

- Behaviour is fully captured by abstract model
- Kernel never fails, behaviour is always well-defined
  - ✓ assertions never fail
  - ✓ will never de-reference null pointer
  - ✓ will never access array out of bounds
  - ✓ cannot be subverted by mis-formed input
  - ✓ …

Can prove further properties on abstract level!

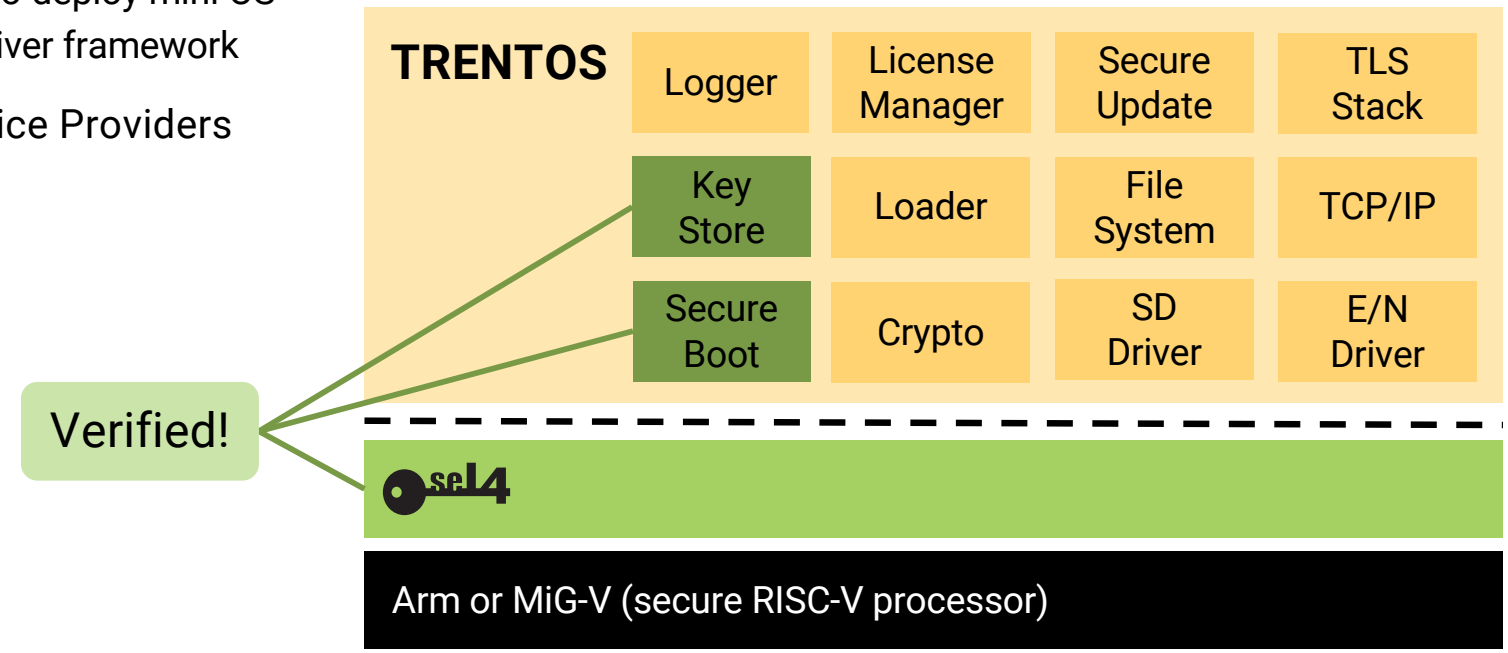
Bugs found:
- 16 in (shallow) testing
- 460 in verification
  - 160 in C,
  - 150 in design,
  - 150 in spec

Verification Cost in Context



But I Need an OS!

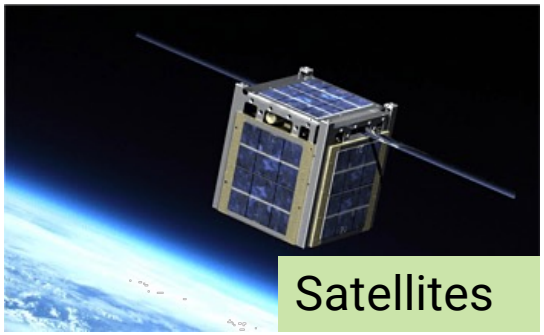
- ✓Many OS components available for free on the seL4 GitHub
- ✓Alternative: HENSOLDT Cyber's TRENTOS†
- ✓Under development (all open source):
  - ✓seL4 Core Platform – easy-to-deploy mini OS
  - ✓secure high-performance driver framework
- ✓Also seL4 Foundation Service Providers



† Disclosure: Conflict of interest

Made For Real-World Use

Autonomous vehicles

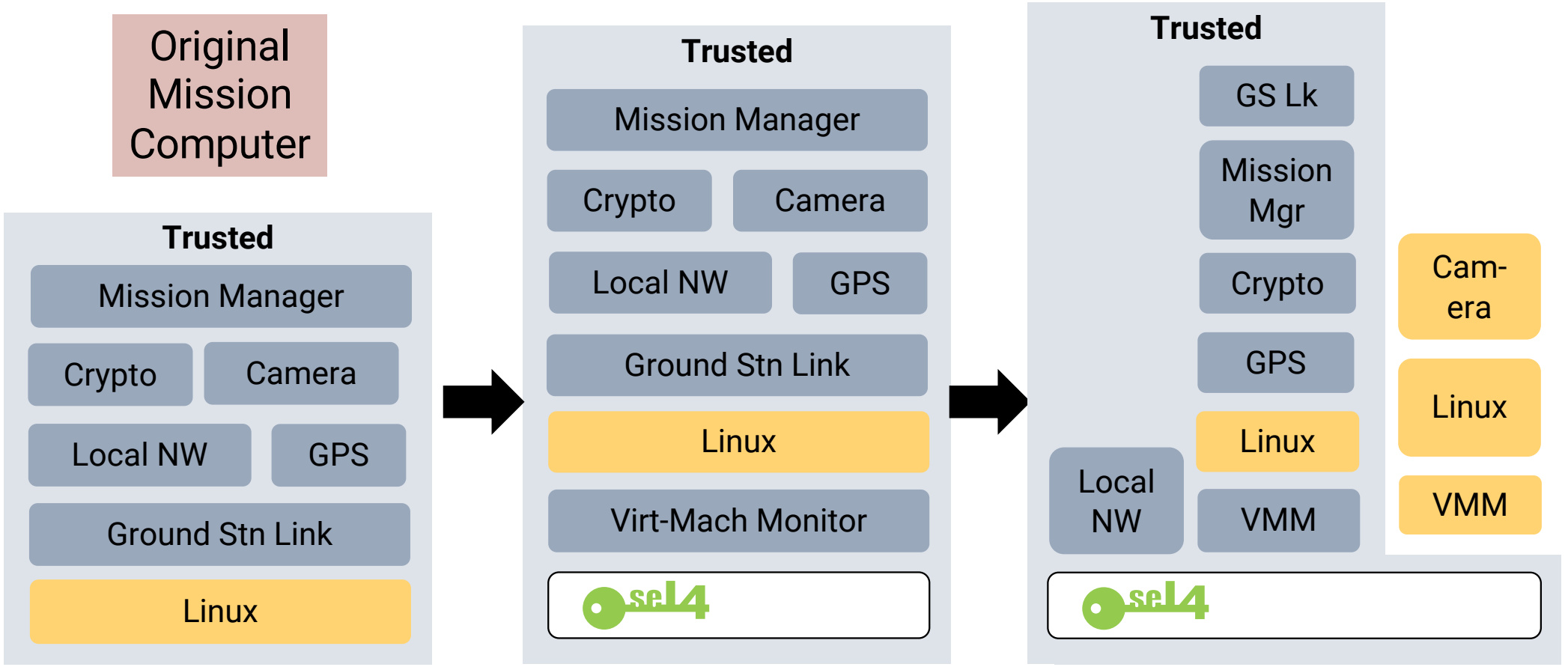


Satellites

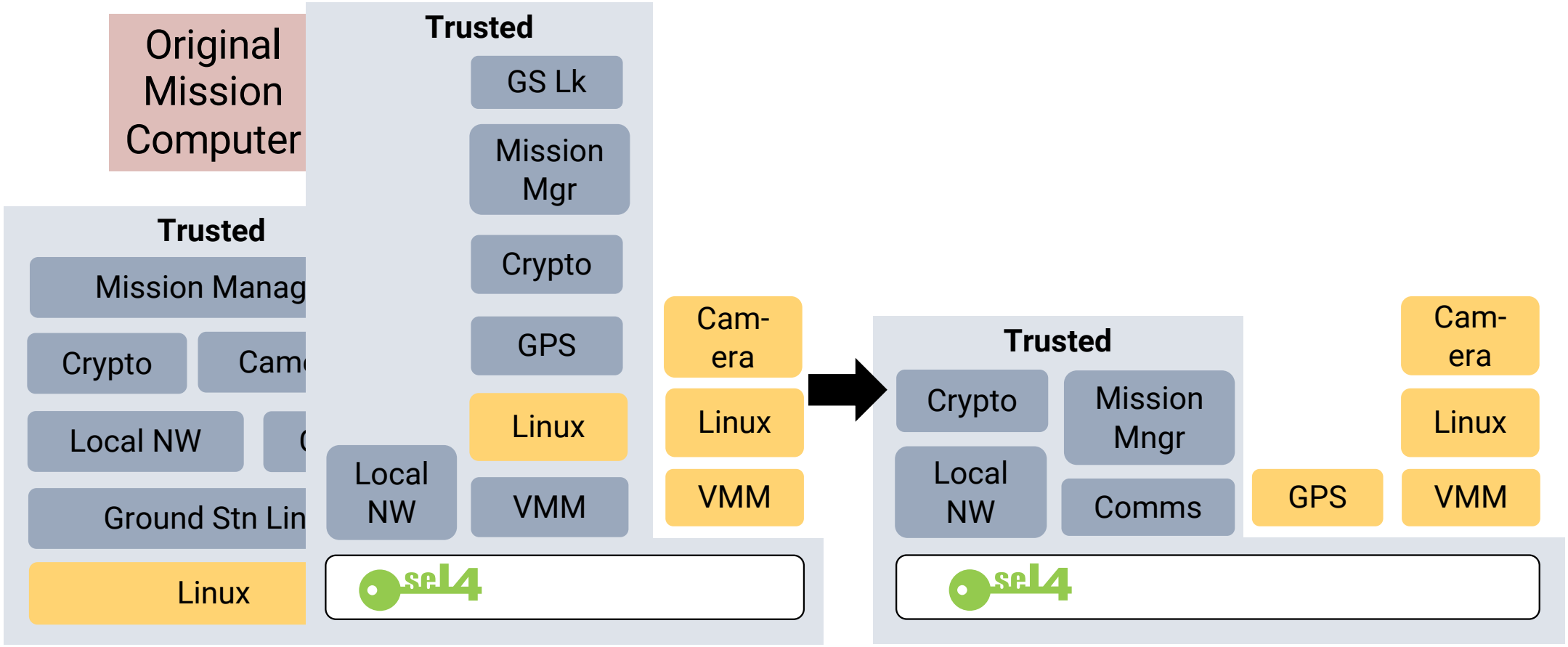
Secure communication device
In use in AU, UK defence forces

Laot: Critical infrastructure protection

DARPA HACMS: Incremental Cyber Retrofit

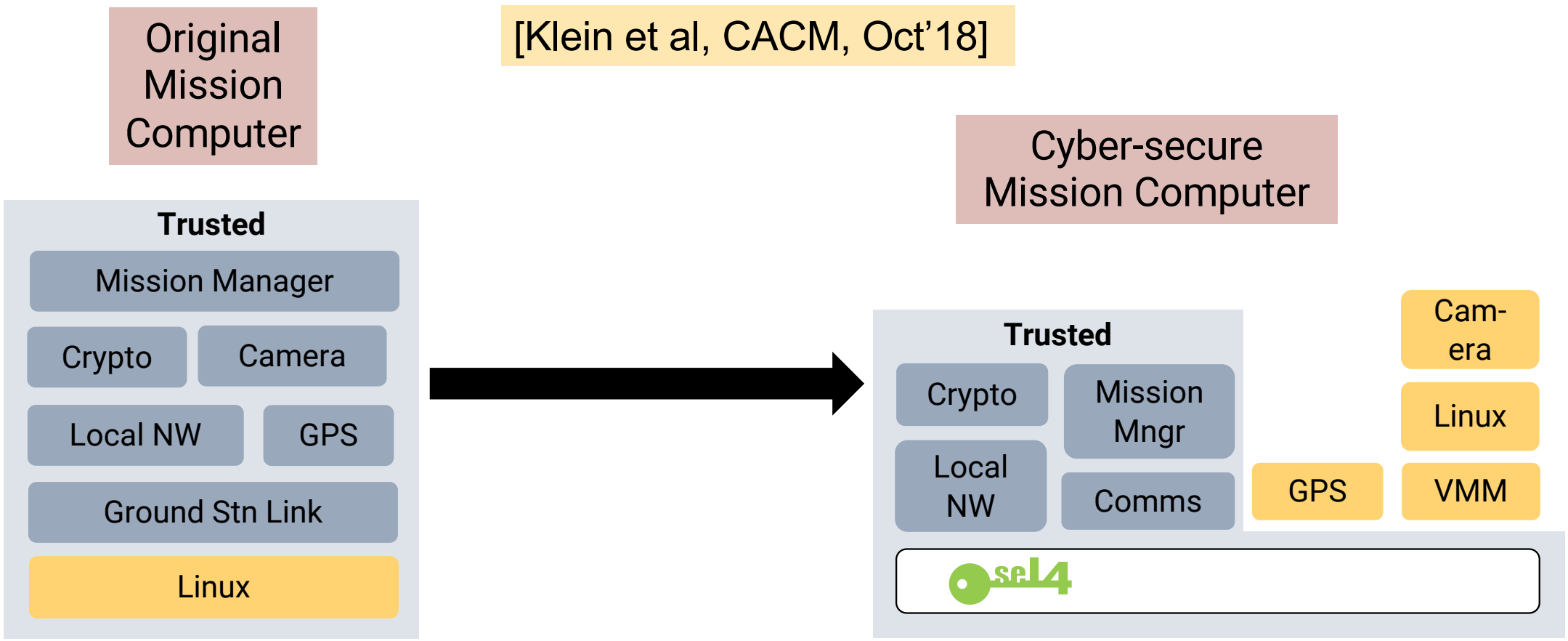


DARPA HACMS: Incremental Cyber Retrofit



DARPA HACMS: Incremental Cyber Retrofit

[Klein et al, CACM, Oct'18]



World’s Most Secure Drone: DEFCON’21

← Tweet

DARPA
@DARPA

We brought a hackable quadcopter with defenses built on our HACMS program to @defcon #AerospaceVillage.

seL4 Foundation

Premium Members

UNSW SYDNEY

Cyber

sel4 FOUNDATION

地 平 线
Horizon Robotics

jumptrading

Li Auto

HENSOLDT
Detect and Protect.

NIO

General Members

Adventium LABS

Coq™

DORNERWORKS

GHOST

KRYIO

LOTUS

penten

Proofcraft

Raytheon Technologies

SECOND STATE

xcalibyte

Associate Members

ETH zürich

KANSAS STATE UNIVERSITY

in association with
National Cyber Security Centre

RISC-V®

TUM

Summary

- Mathematical proof techniques apply to real-world software
- seL4 is a rock-solid basis for security/safety-critical systems

Defining the state of the art
in trustworthy operating systems
for 13 years – and counting!

Further Reading:

- About seL4: https://sel4.systems/
- seL4 whitepaper: https://sel4.systems/About/seL4-whitepaper.pdf
- seL4 Foundation: https://sel4.systems/Foundation