School of Computer Science & Engineering

Trustworthy Systems Group

Securing The Kernel

The seL4® Microkernel

Gernot Heiser

UNSW Sydney & seL4 Foundation

gernot@unsw.edu.au, @GernotHeiser

What is seL4

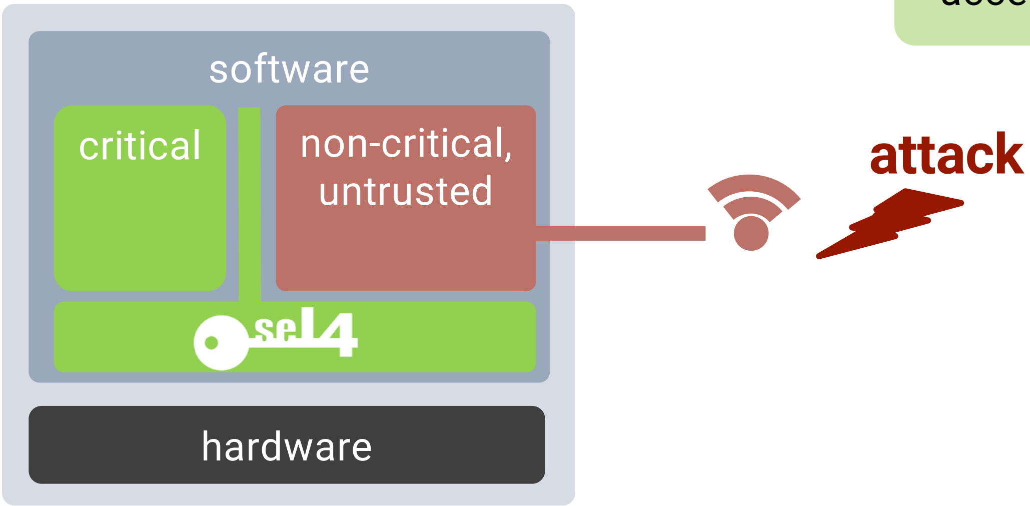
seL4 is an open source, high-assurance, high-performance operating system microkernel

Available on GitHub under GPLv2 license (code and proofs!)

World's most comprehensive mathematical proofs of correctness and security

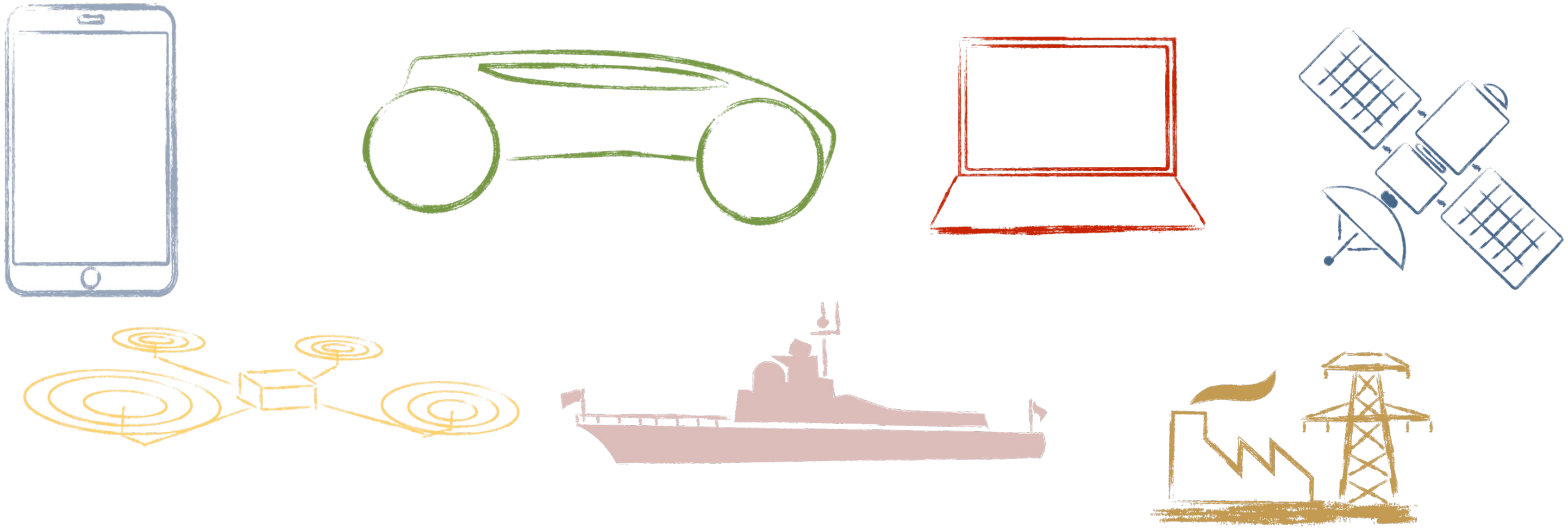
World's fastest microkernel

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



Deployed / in designs across many domains:
automotive, avionics, space, defence, IoT, industry 4.0

seL4 The Benchmark for Performance

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

World's fastest microkernel!

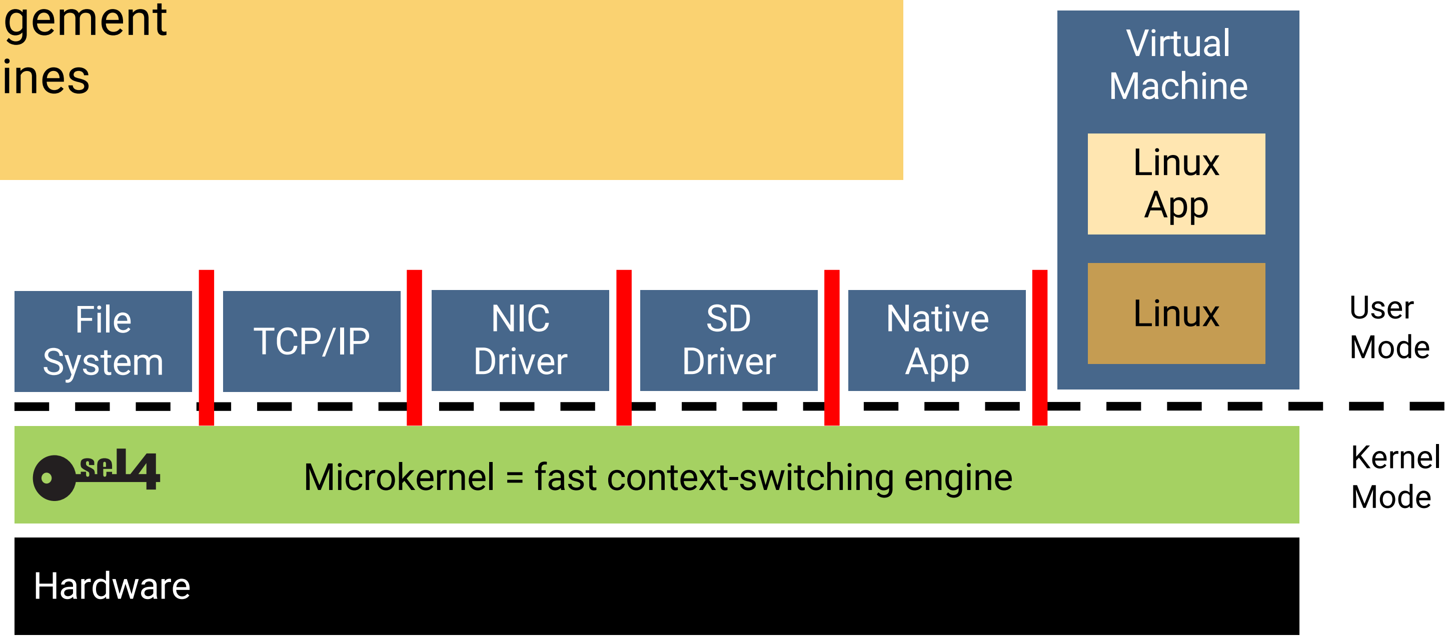
Source	**seL4**	Fiasco.OC	Zircon
Mi et al, 2019	**986**	2717	8157
Gu et al, 2020	**1450**	3057	8151
seL4.systems, Feb'21	**814**	N/A	N/A

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

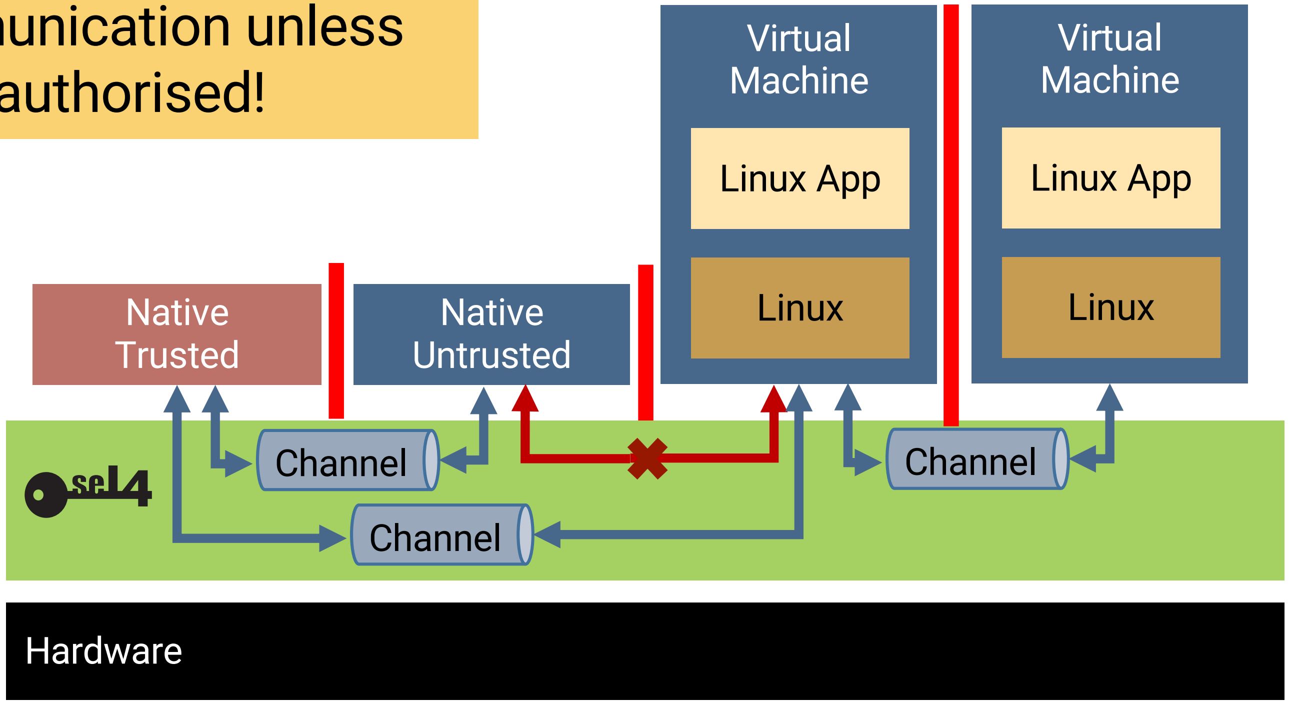
A Microkernel is not an Operating System

All operating-system services are user-level processes:
- file systems
- device drivers
- power management
- virtual machines
- …

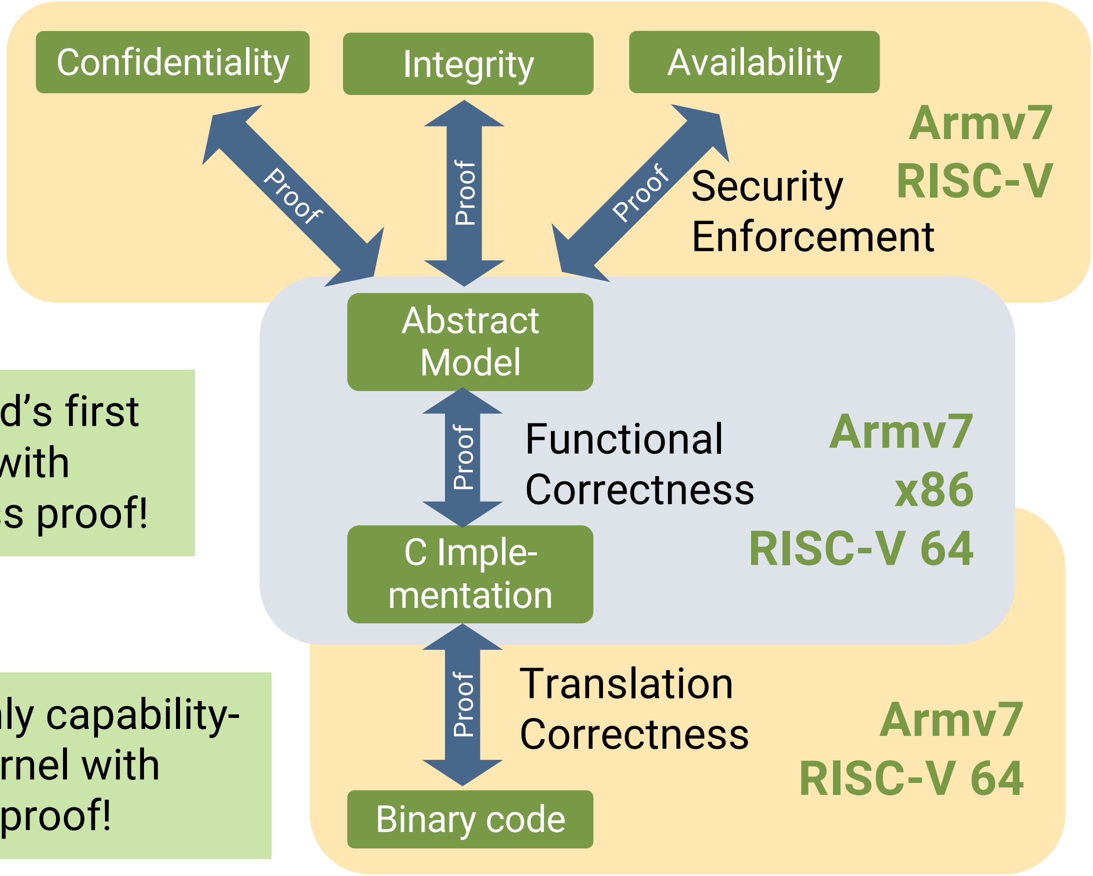


seL4 Capabilities Control Communication

- Fine-grained access control
- No communication unless explicitly authorised!



seL4 Trustworthiness By Mathematical Proof



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

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

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

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

seL4 What Does This Mean?

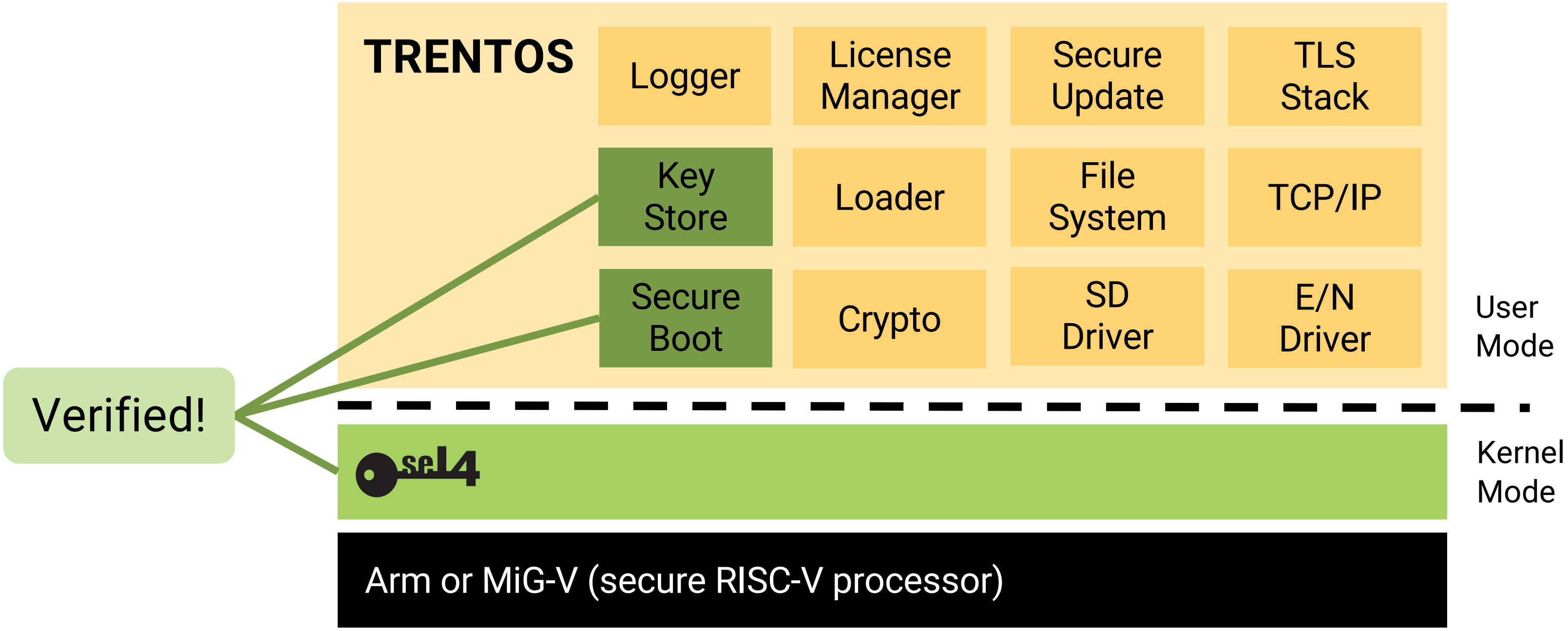
Kinds of properties proved for functional correctness

- 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!

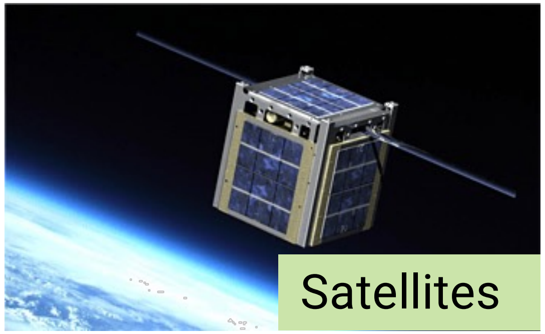
seL4 But I Need an OS!

- ✓ Many OS components available on the seL4 GitHub
- ✓ Alternative: HENSOLDT Cyber's TRENTOS
- ✓ Also seL4 Foundation Service Providers



seL4 Made For Real-World Use

Autonomous vehicles

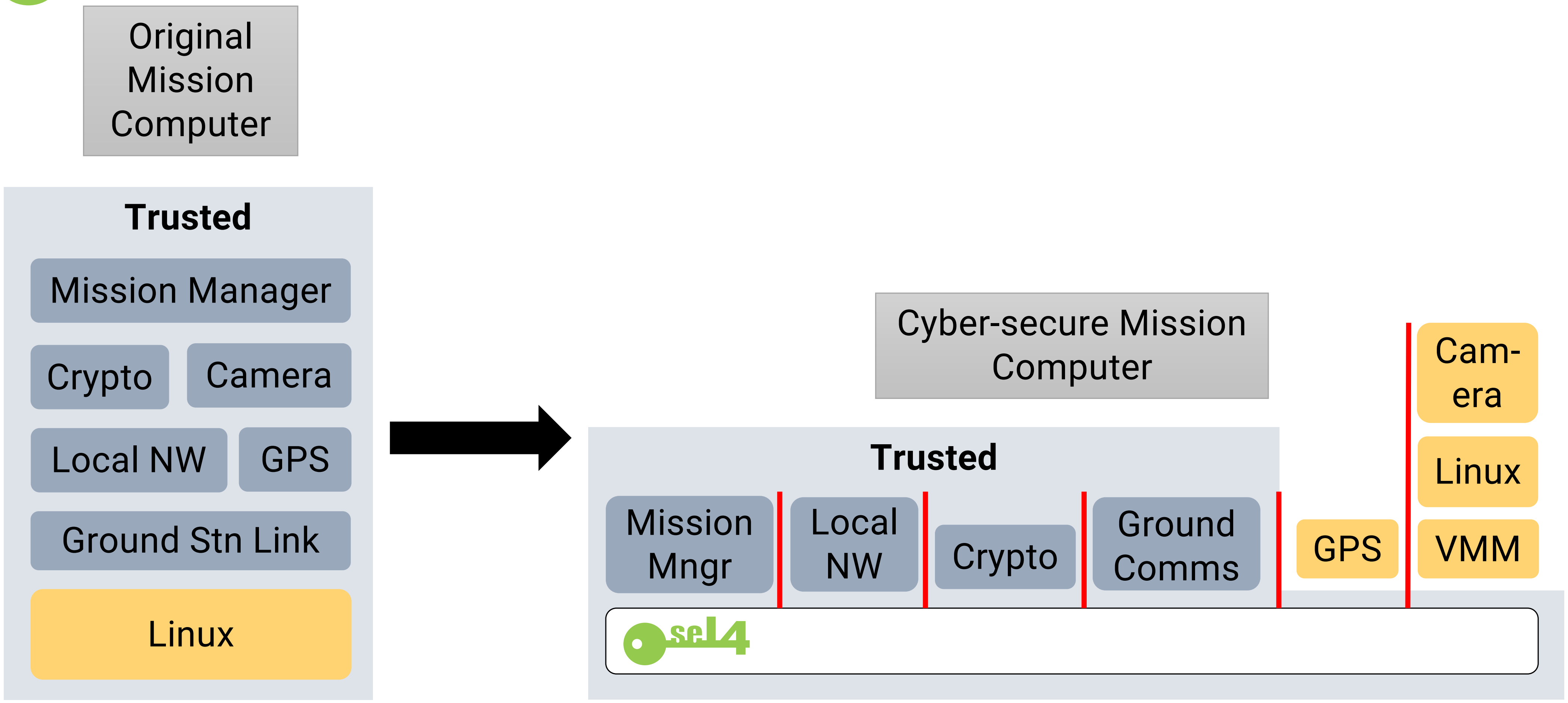


Satellites

Secure communication device
In use in AU, UK defence forces

Laot: Critical infrastructure protection

DARPA HACMS: Incremental Cyber Retrofit



Original Mission Computer

Trusted

Mission Manager

Crypto

Camera

Local NW

GPS

Ground Stn Link

Linux

Cyber-secure Mission Computer

Trusted

Mission Mngr

Local NW

Crypto

Ground Comms

GPS

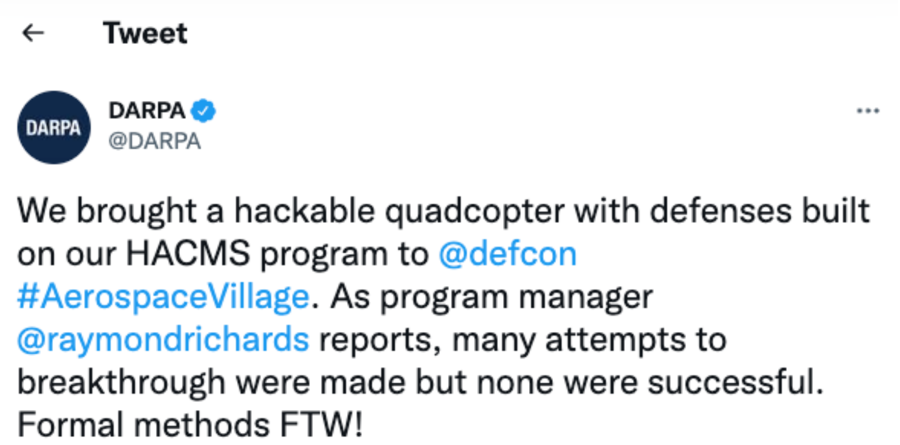
Cam-era

Linux

VMM

seL4

HACMS: World’s Most Secure Drone



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 Foundation

seL4 FOUNDATION

Premium Members

Cyber

UNSW SYDNEY

地 平 线 Horizon Robotics

jumptrading

HENSOLDT Detect and Protect.

Li Auto

NIO

General Members

Adventium® LABS

Cog™

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 can be applied to real-world software
- Provable security is possible – for a well-designed system
- seL4 is a rock-solid basis for security/safety-critical systems

Defining the state of the art
in trustworthy operating systems
for over 10 years

Further Reading:

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