School of Computer Science & Engineering

Trustworthy Systems Group

LionsOS

Fast – Secure – Adaptable

Gernot Heiser

gernot@unsw.edu.au
@gernot@discuss.systems
https://microkerneldude.org/

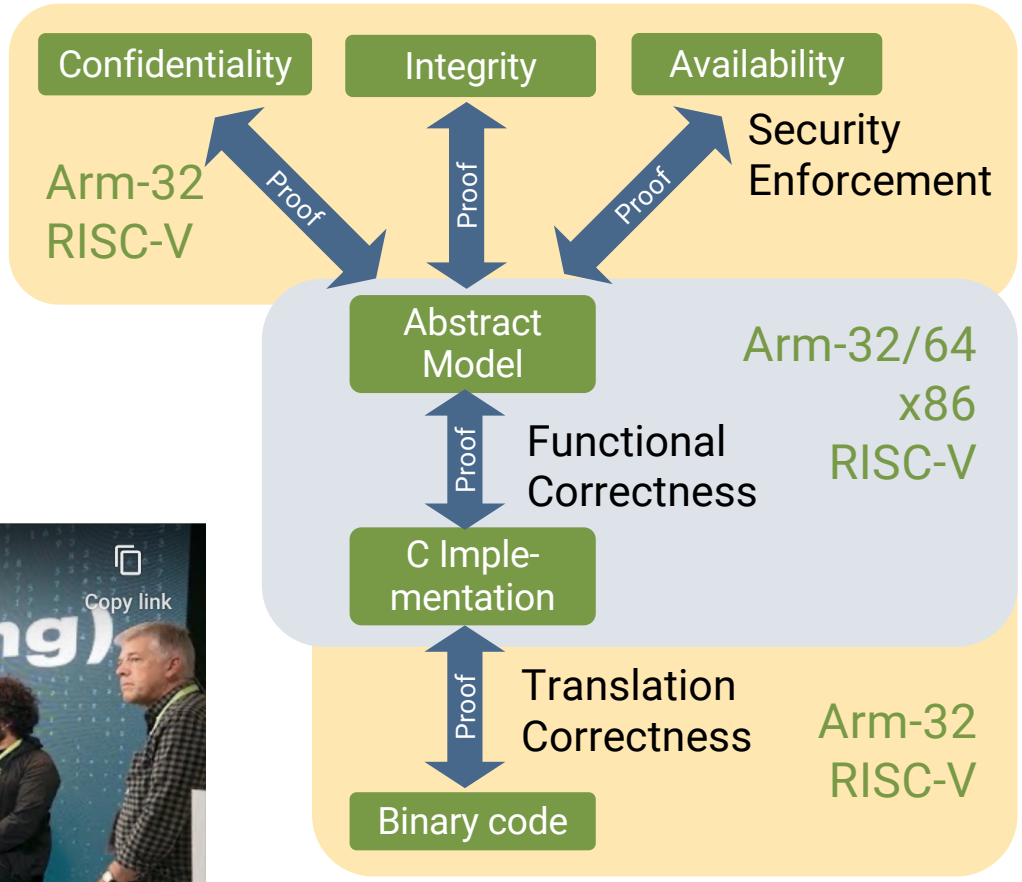
Intrusion Detection

… is an admission of defeat!

We do **intrusion prevention**

Mathematically Proved Secure

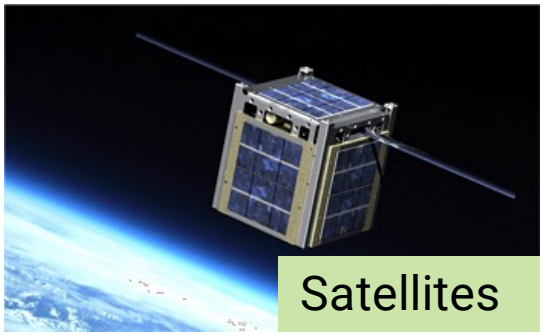
- Complete proof chain from high-level security properties to the binary code
- World's fastest microkernel
- Open source



2022 ACM Software System Award

Used in Real-World Systems

Autonomous vehicles



Satellites

Critical infrastructure protection

Secure communication device
In use in multiple defense forces

Cars

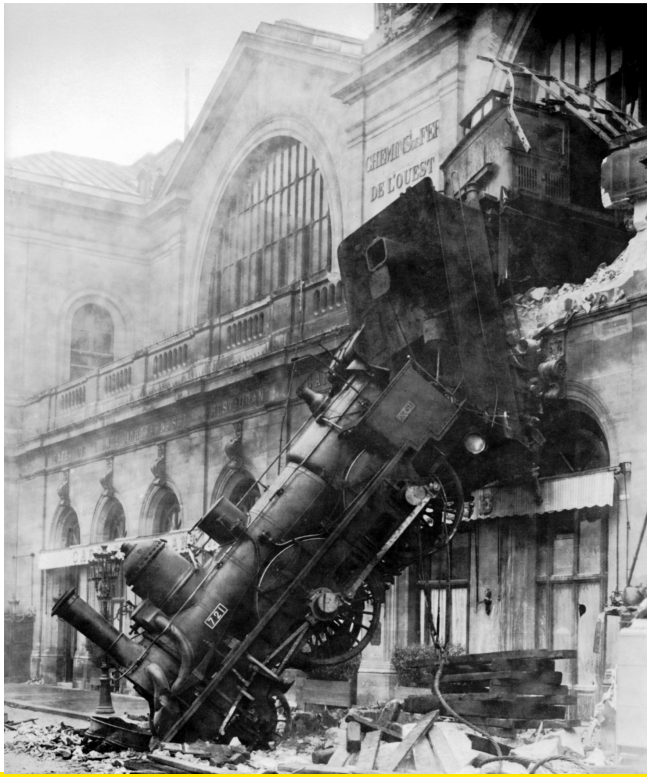
seL4 is Unusuable by Almost Everyone

Good design on seL4 requires deep expertise

Rare beyond TS and ex-TSers

The seL4 community needs an OS that is:

- well designed
- easy to use
- open source



LionsOS Aims

Aim 1: *Practical, easy-to-use, open-source* OS for wide range of *embedded/IoT/cyberphysical* use cases

Can use static architecture

Must be well designed!

Aim 2: *Best-performing* microkernel-based OS ever

Aim 3: *Most secure* OS ever

Must be verified!

Overarching Design Principle: KISS!

LionsOS is what Posix/Unix isn't!

… but we'll have Posix-like I/O wrappers

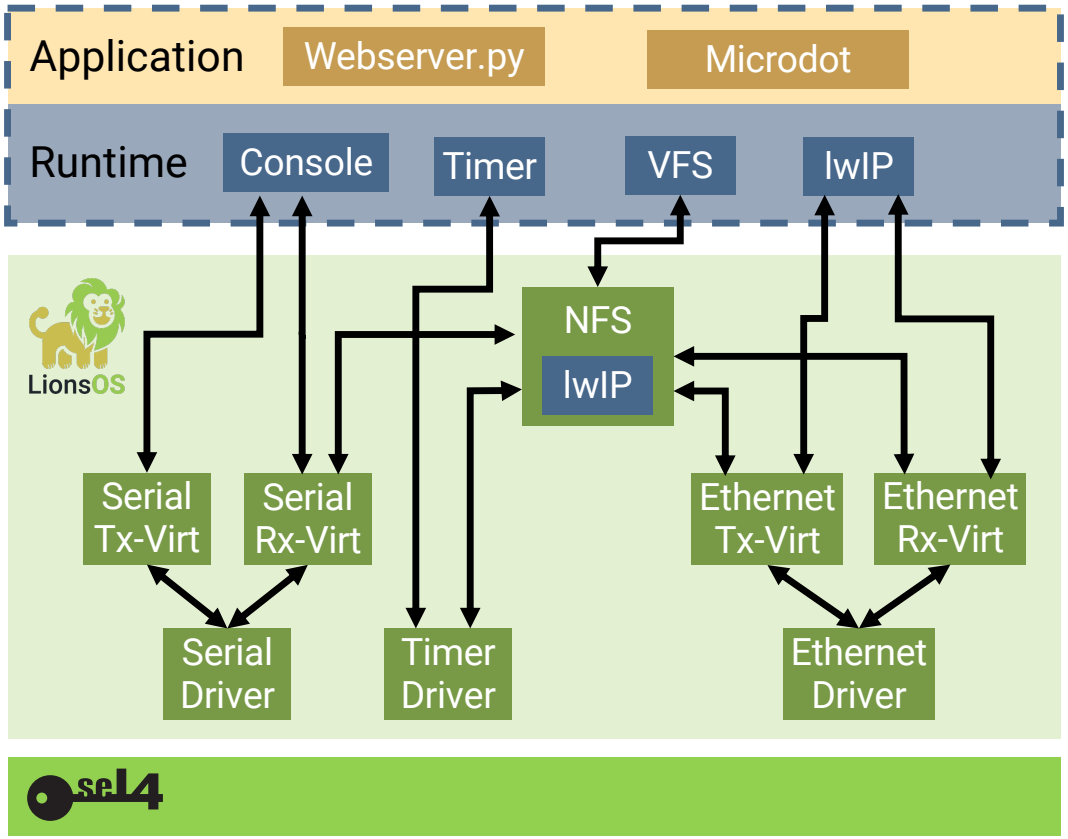
Helps development **and** verification!

Radical simplicity:

- fine-grained modularity, strict separation of concerns
- event-driven programming model
- use-case-specific policies

Use-case diversity by replacing components

Underneath https://sel4.systems/

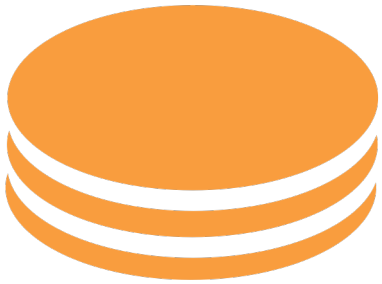


Component	LoC	Library	LoC
Serial Driver	249	Microkit	303
Serial Tx Virt	175	Ser. queue	219
Serial Rx Virt	126	I2C queue	101
I2C Driver	514	Eth queue	140
I2C Virt	154	FS queue & protocol	268
Timer Driver	136		
Eth Driver	397	Coroutines	848
Eth Tx Virt	122	LWIP	16,280
Eth Rx Virt	160	NFS	45,707
Eth Copier	79	VMM	3,098

Untrusted

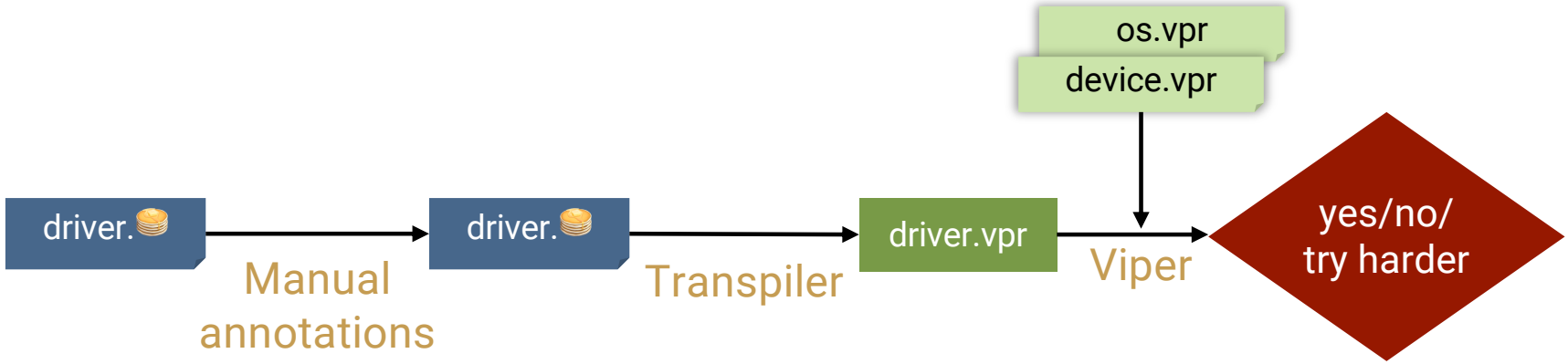
TCB: 3.1 kSLOC

Verification: Ethernet Driver

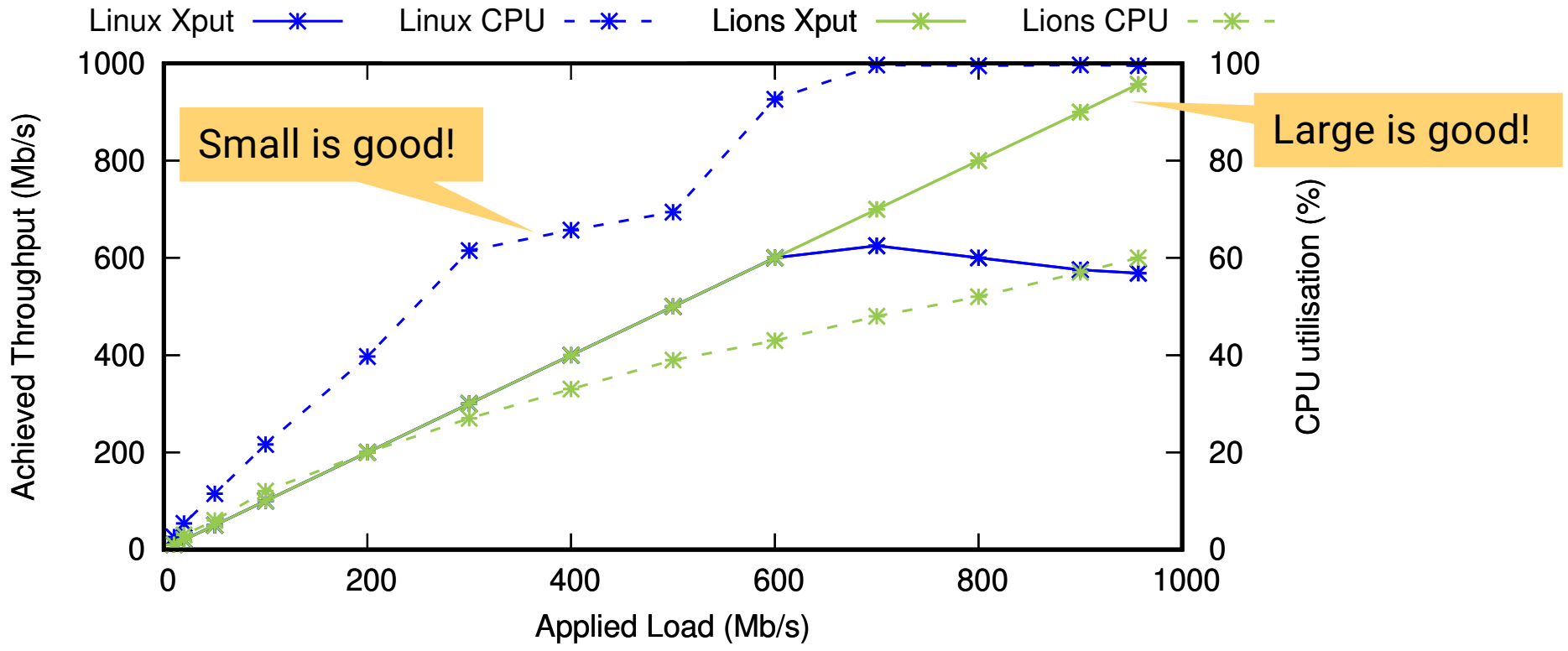


PANCAKE

- C-like, systems-programmer friendly
- Verified compiler!
- Successfully verified real-world Ethernet driver

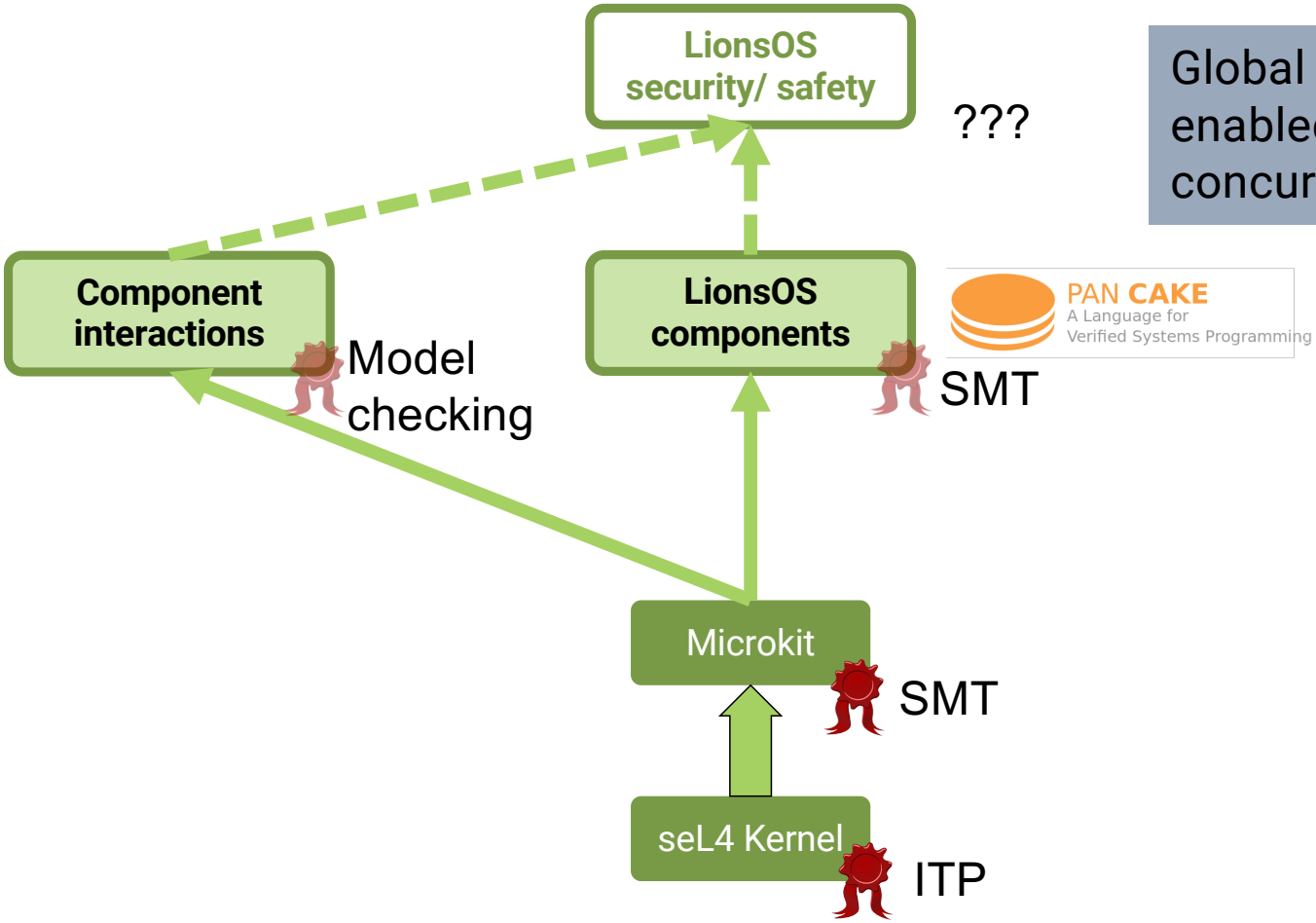


Performance: i.MX8M, 1Gb/s E/N, UDP



Single-core configuration

Verifying Lions OS



Global verification enabled by “tamed” concurrency

https://trustworthy.systems

Security is no excuse for bad performance!

https://trustworthy.systems