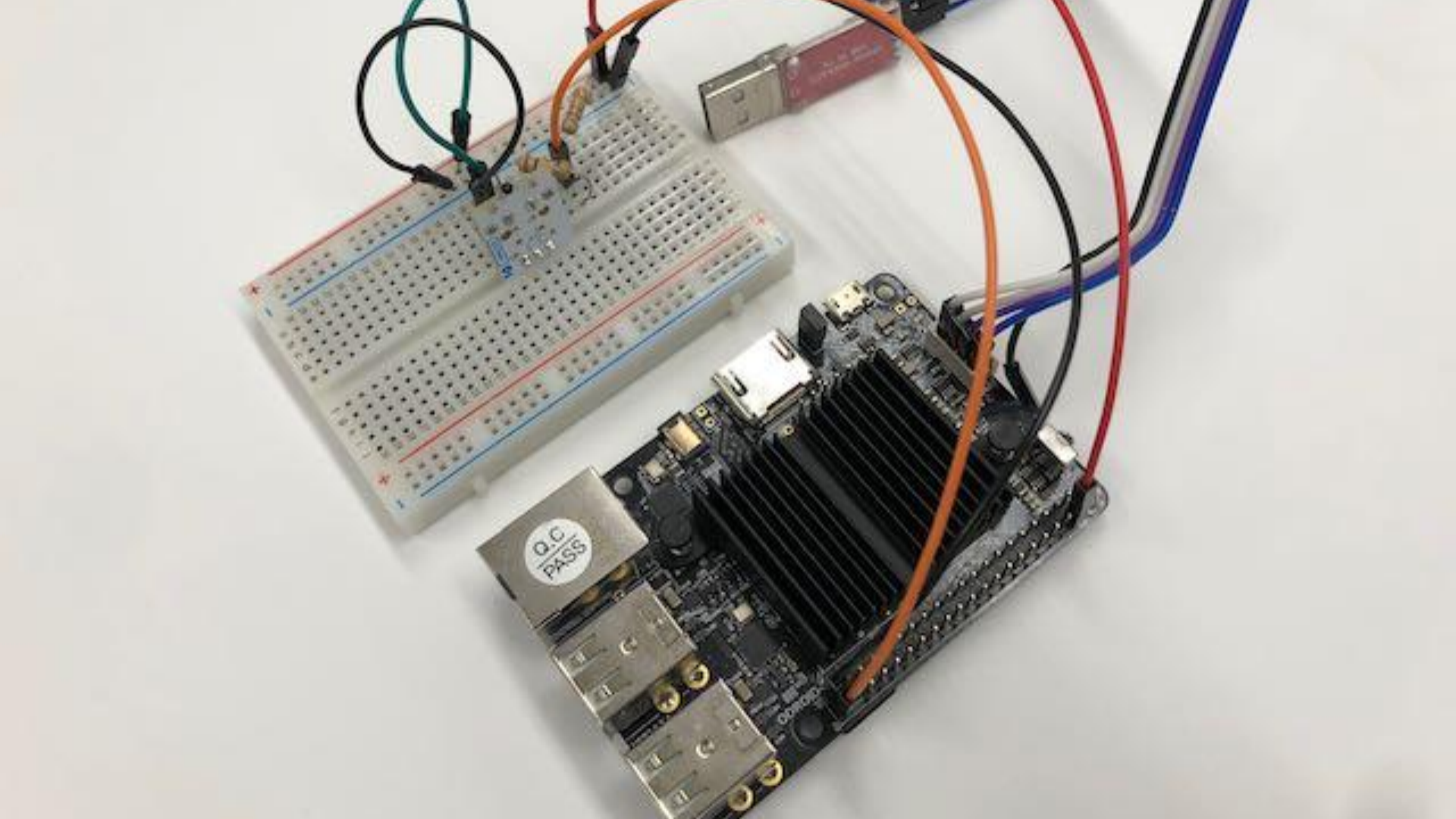
Toward a Verified, Minimal IPv6 Network Stack Implementation

Wyeth Greenlaw Rollins,† Alain Kägi,† Caitlyn Wilde,† Aubrey Birdwell,‡ Richard Weiss,‡ Jens Mache†

†Lewis & Clark ‡Evergreen College

[Szelei Robert, CC0 Public Domain]

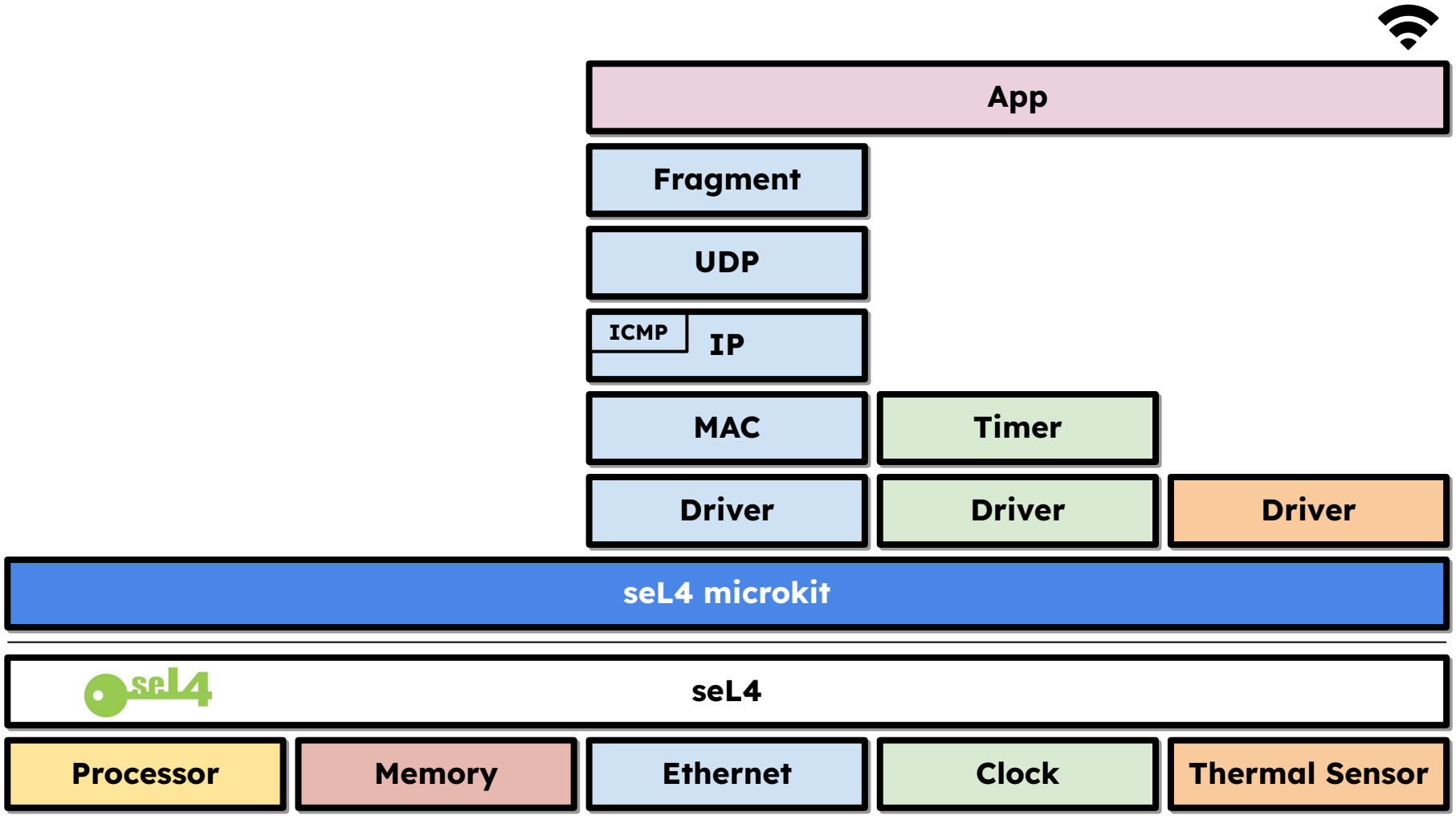

Q.C
PASS

Goal & Approach

- Verified networking stack
- Interactive theorem proving (Isabelle/HOL)

Principles

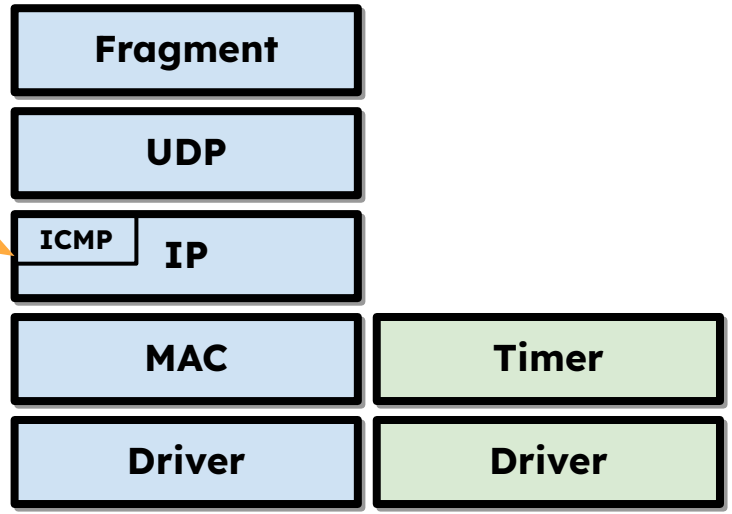
- “Security is not an excuse for poor performance”
  - C
  - Zero copy
  - Bounded buffers
- Separation of concerns
  - “Communicating sequential processes”


App
Fragment
UDP
ICMP
IP
MAC
Timer
Driver
Driver
Driver
seL4 microkit
seL4
Processor
Memory
Ethernet
Clock
Thermal Sensor

- “ping” test
  - Linux raw socket
  - All layers but network driver (using Linux’)
    - In particular, ICMP
      - Echo request
      - Echo reply

IP

Zero copy
Headroom for header
Validation checks



ICMP

Error and management

(Error reporting, ping)

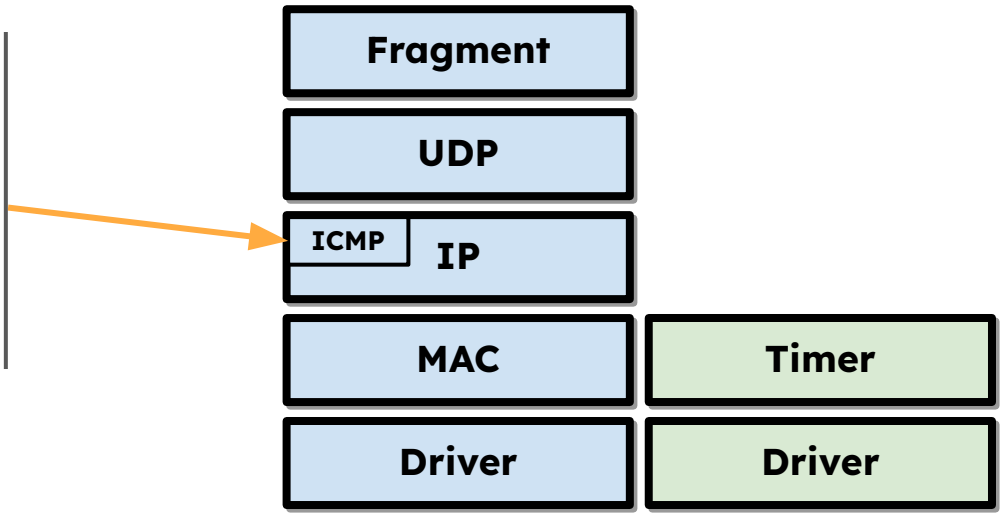
Timer service

Neighbor discovery

(Red-black tree, Nipkow's)

State machine

`bitfield_gen.py`



Status

- Code is complete
  - Echo request and reply
- Verification in progress
  - Fragmentation & reassembly
- Tested on Odroid-C2, imx8mm-evk

Questions