TruSDEd: Trustworthy, Software-Defined Cyberattack Detection and Mitigation at the Network Edge

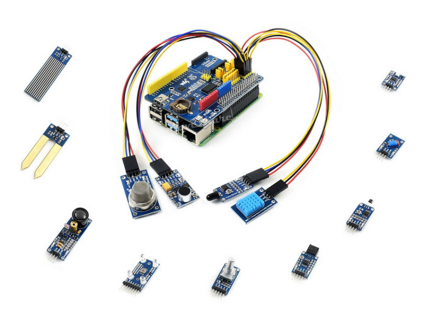
Kyle A. Simpson, Chris Williamson, Douglas J. Paul, Dimitrios P. Pezaros
`k.simpson.1@research.gla.ac.uk`
FelixMcFelix `https://mcfelix.me`

PETRAS Ops Meeting, 19 July 2022

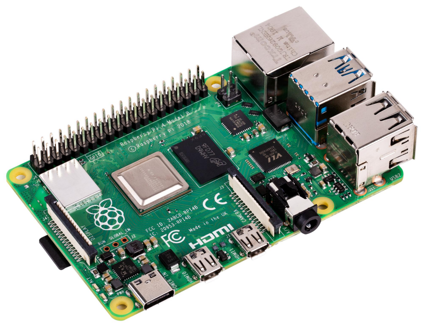
University of Glasgow

Securing Sensor & IoT Networks

- Security – ingress/egress packet processing by *network functions*.
    - IP layer – Firewalls, DPI, ACLs...
    - Middleboxes a bad fit.
    - Needs to be reconfigurable – attacks and security context evolve.
- Ideally in-situ.
    - Dynamic/retrofitted.
    - But limited space + power in the field.
    - Physically vulnerable!



Fast, cheap, and secure IoT Defence – pick 3?



- Single-board compute like RPis are small, capable, affordable! Cheap!
    - See also: NUCs, Jetsons.
- Sensor networks have low data rates; a good fit.
- Project goals:
    - Fast! Low-latency, quickly reconfigurable.
    - Secure! *Device*-level authentication.

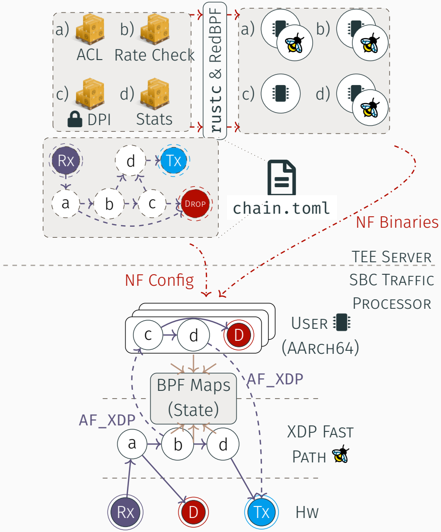
Research Objectives

- Fast reconfiguration:
    - State, Program Code, Composition
- Attestation and authentication:
    - Right programs on right machine, requested by trusted server.
- ‘Acceptably’ low-latency packet-processing, without pushing CPU/power draw too high?
    - I.e., as low as we can get without polling.
- Easy development and composition.
    - One Rust program per NF $\implies$ compiled for stack.
    - Simple, dynamic chain format.

Limits of existing solutions

- ‘Best’ low latency processing (DPDK) is expensive – CPU and power.
    - …IFF you have HW support (NUCs)
- SotA in *secure* processing needs server-only capabilities like *trusted execution environments* (TEEs).
- No powerful hardware offloads or acceleration.
    - FPGA hats/daughterboards ‘off-path’
- Devices physically vulnerable, no ECC memory.
- …So, how to reconcile with cheap & portable SBCs?

Methodology (I): Low-latency XDP fast-path



- Two-tier approach—XDP & User.
- Composable NFs – graph structure.
- Critical or high performance NFs go into XDP:
  - Early results – low latency for most packets.
- Rare 'slow-path' still kernel bypass:
  - Expensive & proprietary code.
  - Only for candidate attack traffic.
- Reconfigurable, dynamic.

Methodology (Ia): Low-latency XDP fast-path

- Consistent NF API for both XDP/userland.
- Rust compiler enforces…
  - *#![forbid(unsafe_code)]* on NF module crates,
  - all NF branches specified.
- All compilation on TEE-equipped server.
  - SBC too constrained.
  - Can attest compiler etc. following SotA!

```rust
#![no_std]
#![forbid(unsafe_code)]
pub enum Action {
    Left,
    Right,
    Up,
    Down,
}

// Some len checks omitted.
pub fn packet(bytes: &mut [u8]) -> Action {
    let addr_lsb_idx = 14 + match &bytes[12..14] {
        &[0x08, 0x00] => 19, //v4
        &[0x86, 0xDD] => 39, //v6
        _ => {return Action::Left},
    };

    match bytes[addr_lsb_idx] % 2 {
        0 => Action::Left,
        1 => Action::Right,
        2 => Action::Up,
        3 => Action::Down,
        _ => unreachable!(),
    }
}
```

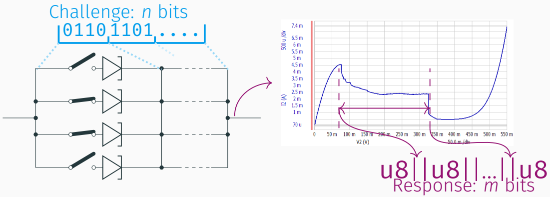
mod.rs: Load balance on dest addr

Methodology (II): Novel PUF-based authentication

- How to attest the above code and config is correct?
  - TLS w/ pre-shared certs works well.
  - But corruption possible on field devices (no ECC).
- *Physical Unclonable Functions* (PUFs) – input-based device signatures, CRPs.
- Authenticate keys in the wild without root certs.
  - Two-way: Client $\leftrightarrow$ Server!
  - Goal: Adapt PQC TLS variants for these PUF certs.
- Strong attestation of identities to physical devices.

Methodology (IIa): Novel PUF-based authentication

- RTD-based array designs – quantum property.
- Behaviour in purple region (NDR region) physical device-dependent
  - Perturbations from ‘ideal’ behaviour can’t be replicated
  - N° peaks and perturbations depend on active devices.
- Challenge bits control used transistors in circuit
  - $\sim$ Exp amount in n, Large Resp.



Takeaways:

Cheap NFs: SBCs for packet processing.

Low-latency and fast: XDP path for majority of traffic, early & cheap anomaly checks.

Secure: PUFs for device, server, and function chain attestation.

Ongoing work: complex NFs, power + latency measures, adapting RusTLS, better characterising PUF behaviour.

Questions?

University of Glasgow

k.simpson.1@research.gla.ac.uk

FelixMcFelix https://mcfelix.me

NETLAB
NETWORKED SYSTEMS RESEARCH LABORATORY
University of Glasgow | School of Computing Science