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

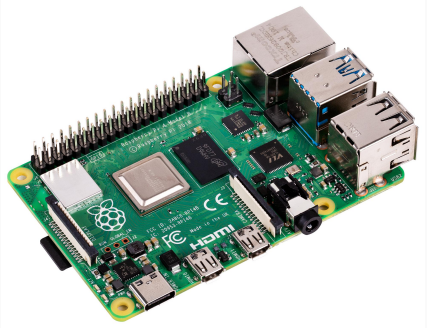
Kyle A. Simpson, Chris Williamson, Douglas J. Paul, Dimitrios P. Pezaros
k.simpson.1@research.gla.ac.uk
FelixMcFelix https://mcfelix.me

PETRAS Academic Community Conference, 16–17 June, 2022

University of Glasgow

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

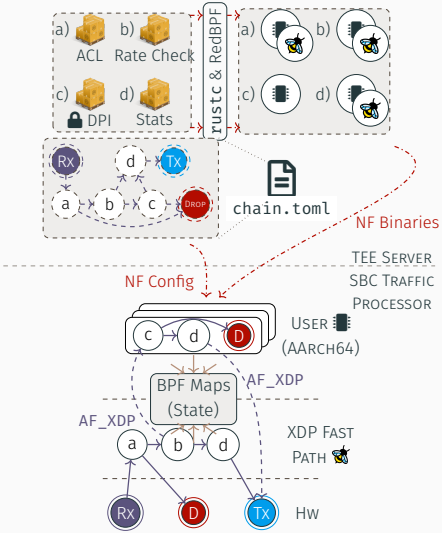
- Security – packet processing by *network functions*. Firewalls, DPI, ACLs...
- Ideally in-situ.
- Single-board compute like RPis are small, capable, affordable!
- Sensor networks have low data rates; a good fit.



Challenges

- ‘Best’ low latency processing (DPDK) is expensive – CPU and power.
- SoTA in *secure* processing needs server-only capabilities like *trusted execution environments* (TEEs).
- No powerful hardware offloads or acceleration.
- Devices physically vulnerable, no ECC memory.
- ...So, how to reconcile with cheap & portable SBCs?

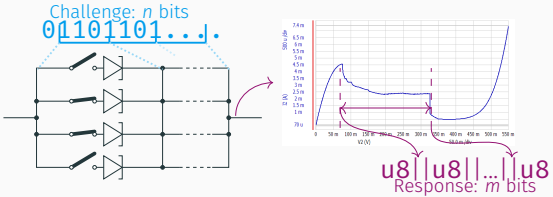
Methodology (I): Low-latency XDP fast-path



- Two-tier approach.
- 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.

Methodology (II): Novel PUF-based authentication

- How to attest the above is correct?
- Physical unclonable functions (PUFs) – input-based device signatures, CRPs.
- Authenticate keys in the wild without root certs.
- Strong attestation of identities to physical devices.
- RTD-based array designs – quantum property.



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: integrating userland functions, state management, 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