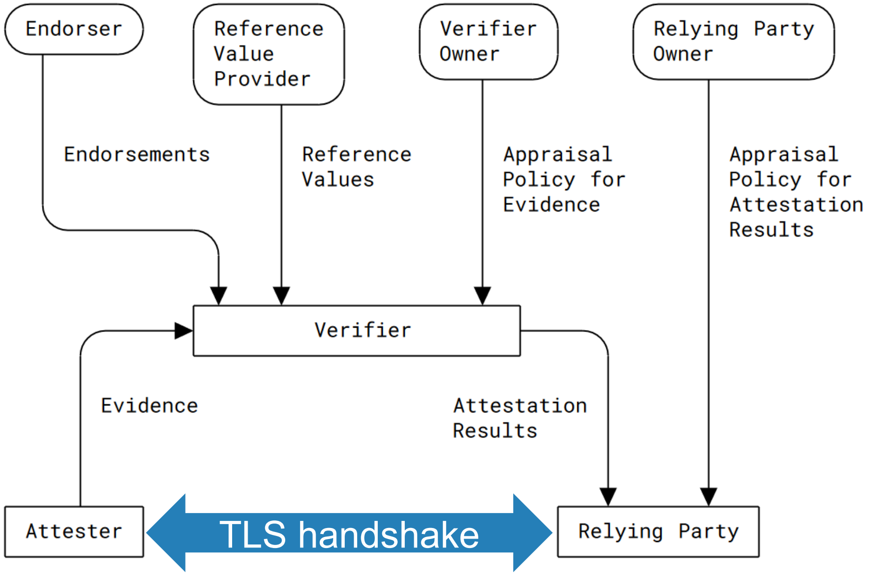
Linaro Connect
MADRID 2024 | MAY 14-17 2024

mbedTLS prototype

Present and future

System architecture (recap)

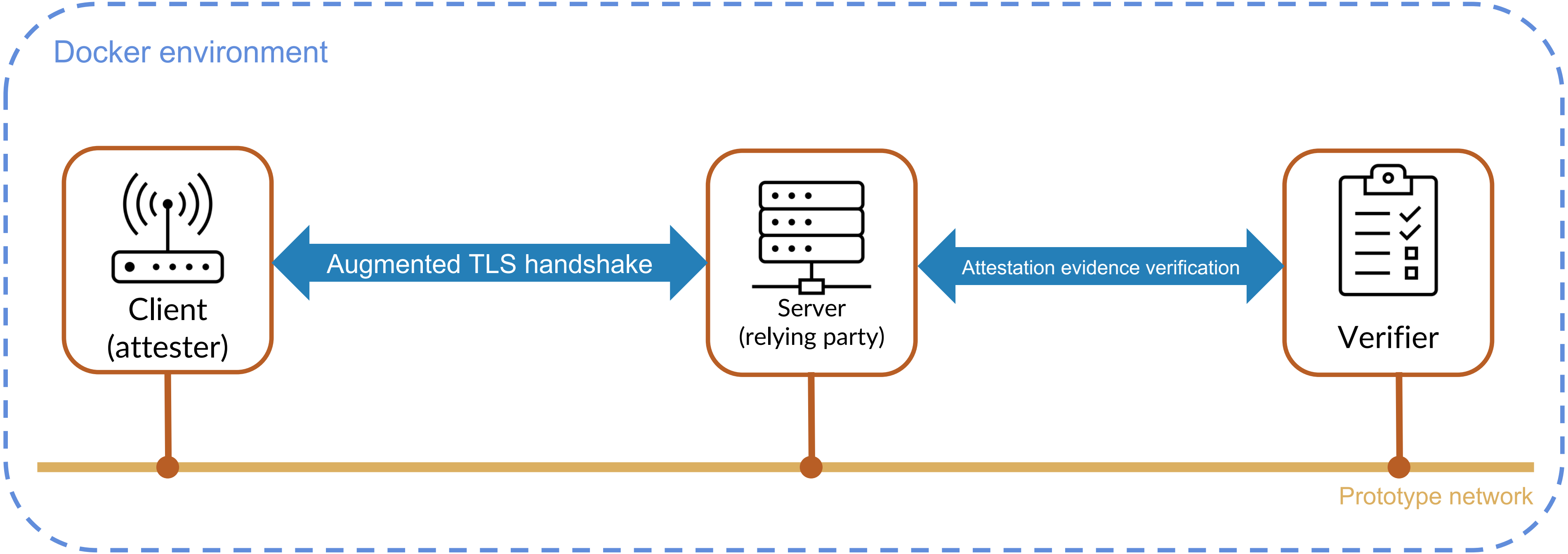


Flexibility of design

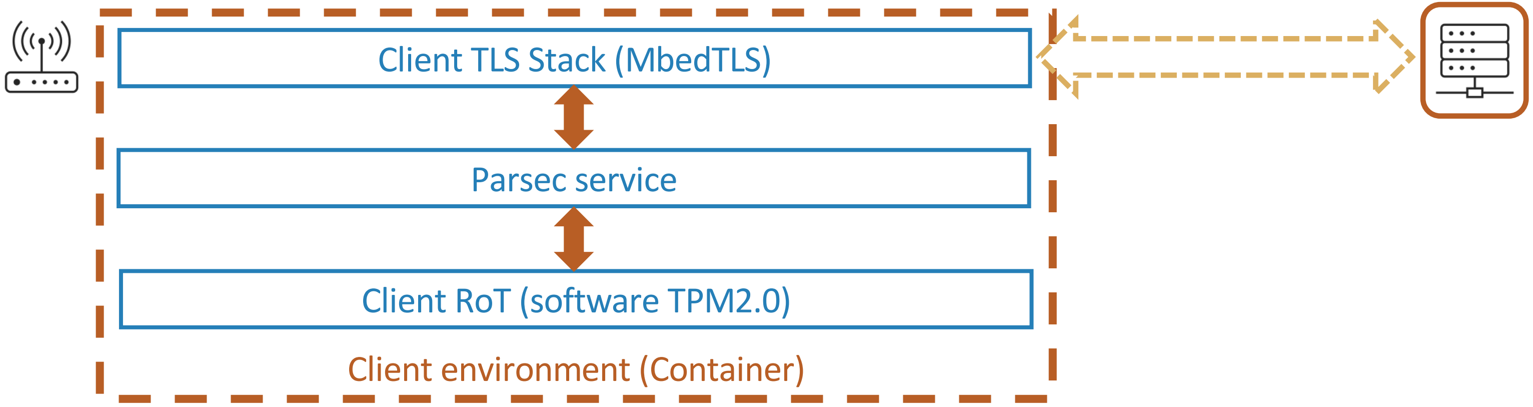
- Both peers can use attestation to authenticate themselves
  - Any Root of Trust (RoT) should be usable
- Both attestation evidence and results can serve as credentials
- Attestation credentials can be used alongside, or as a replacement to PKIX

- The explosion of options makes a comprehensive prototype costly to implement
  - We chose to support one such configuration to begin with

Prototype architecture



Client (attester)

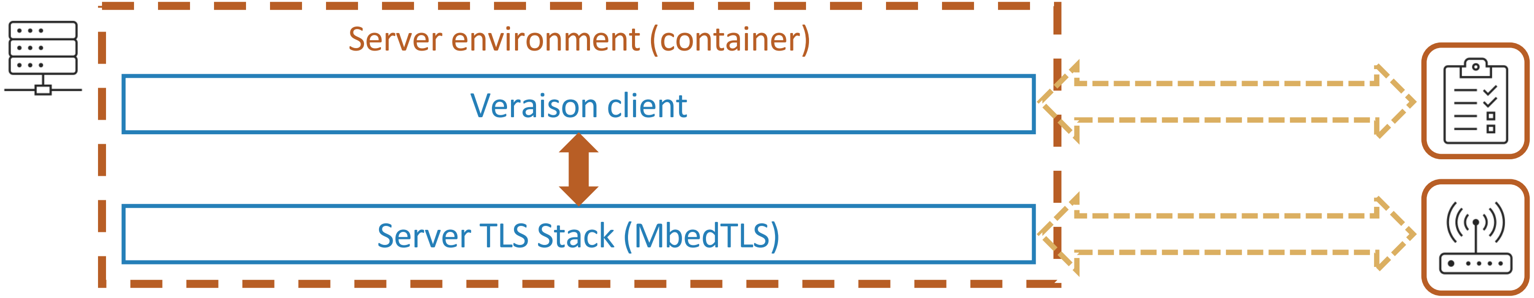

Client TLS Stack (MbedTLS)

Parsec service

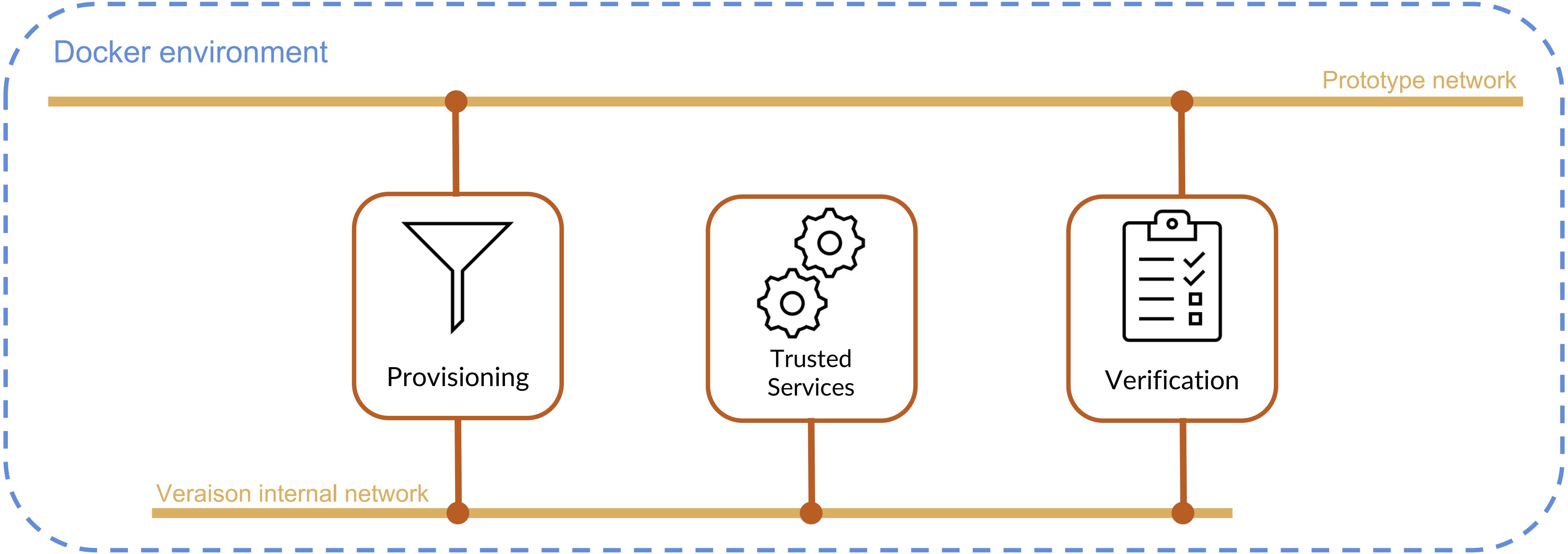
Client RoT (software TPM2.0)

Client environment (Container)

Server (relying party)



Verifier


Docker environment
Prototype network
Provisioning
Trusted Services
Verification
Veraison internal network

Current problems and limitations

- Build process for container images has a history of blowing up
- Some Veraison interfaces have been shifting underneath our feet
- mbedTLS server relies on a cert that has expired

- Negotiation isn’t properly supported
- Significant features are not supported (e.g., passport model)
- No benchmarking framework available

Plans for the future

- Add support for more Roots of Trust (e.g., CCA)
- Get some benchmarking figures
- Use different TLS stacks for client and server
- Upstream (some of) the patches we’ve made

Thank you

Attested TLS PoC repo