Attendees: Kevin Townsend (Linaro), Don Harbin (Linaro), Joakim Bech (Linaro), Dan Handley (Arm), Shebu Varghese Kuriakose , Lionel Debieve (ST), Matteo Carlini (Arm), David Brown (Linaro), Julius Werner (Google), Dave Rodgman (Arm), Michael Thomas (Renesas)

Minutes:

- Joakim presented DICE overview - See slides
    - DICE is getting traction with Linaro members and other companies Linaro's been speaking to
    - DavidB: How much of the fw is included in the hash?
        - BL1 requires CDI containing the first mutable code.
        - After use, this can be discarded so it's not accessible by other components
        - There's more flexibility in what is included in subsequent layers
    - DavidB: It seems there's a trade-off between what is measured and how updateable it is
        - Can't change immutable measurement in layer 0. Can change measurements in other layers (assuming they're updateable).
        - Whoever is verifying layers will need to update what they're verifying against
    - Lionel: About the engine, we have the choice of using our own non-TF-A BL1 (ROM), so would we need to manage this part ourselves?
        - Yes, that's necessary in production systems.
        - For prototyping, we can fake something in QEMU
    - LionelD: So it's not very updateable?
        - Yes, for layer 0
    - DICE seems to have good and bad aspects. That's why we've proposed it as a prototype.
        - https://linaro.atlassian.net/browse/TS-295
- Dan talked about Arm's view on DICE:
    - We're also seeing industry traction with this
    - DICE is a very broad architecture. There are also profiles, providing more specific use-cases
        - e.g.https://pigweed.googlesource.com/open-dice/+/HEAD/docs/specification.md
        - That enables attestation and sealing use-cases.
    - Seems to be an expensive technology for low-end devices
    - SW implementation of DICE layers has a potentially large attack surface. Secrets are distributed across layers.
    - Arm is investigating the implementation of an Open DICE service in the Runtime Security Subsystem (RSS) (the SW is part of TF-M)
    - This has better security properties, e.g. isolated secure storage, fault injection protection, etc…
    - We mentioned RSS previously in the context of Arm CCA enablement
    - TF-A BL1/BL2 would be clients of that service
    - Less sure about implementing in TF-A but have no problem if others want to contribute this

- Back to Joakim:
    - Not yet proposing putting in TF-A. Just a prototyping activity
    - We think this could be used for device identification in TF-A, but still working through the use cases.
    - Need feedback from member companies.
    - From OSFC - Presentation from Jorgan Hand: Protecting TPM commands from active interposers:
        - https://www.osfc.io/2022/talks/protecting-tpm-commands-from-active-interposers/
        - That talked about leveraging DICE to generate alias key, which could be used to check for man in the middle attacks
    - Less clear how data will be used by verifier - could have work to isolate attack sources
    - End to end use cases critical to determine what to implement/prototype
- Dan: Hope to be able to share more in the coming months.
- Joakim/Dan open for members to reach out if want 1:1 conversations

- Shebu - Roadmaps Mbed TLS, PSA Crypto overview - See slides
    - Plans to move internal Mbed TLS Arm CI to TF Open CI
    - Mbed TLS running - still working thru some performance issues
    - Lack of visibility of Arm CI was one of the big issues for partners
    - Joakim: Any numbers on BIgNum performance?
        - Improvements in ECC performance have been held back until BigNum refactoring complete
        - DaveR: Expect to get some numbers early next year
    - Project Matter uses OpenThread, which needs ECJ-PAKE support in PSA Crypto API
    - Main TLS1.3 features requested by partners already implemented
        - May go slow on remaining TLS 1.3 features unless there's a clear ask for them
    - Welcome ideas/contributions for memory optimizations
    - New PSA Crypto features has increased code size so want to address this
    - EdDSA is important for constrained devices. Significant part of that already contributed in PR.
    - Mbed TLS has a long backlog. Have a significant number of community contributions needing review.
        - DavidB helping (thanks). Other help gratefully received.
    - Members encouraged to attend the Mbed TLS/PSA crypto weekly calls.
        - Calendar invites here: https://www.trustedfirmware.org/meetings/
        - Subscribe to the maillists here:
            - MBed TLS maillist
            - PSA Crypto Maillist
- Dan AOB:
    - New TF-RMM component released! A blog forthcoming
    - F/W Handoff spec is also now public
    - TF-A LTS is funded for the next year.
        - Looking to get support for 5 year commitment
    - Don will send notes from the board shortly (containing above items)