Attendees: Ilias Apalodimas (Linaro), Gyorgy Szing (Arm), Antonio De Angelis (Arm), Kevin Oerton (NXM Labs), David Brown(Linaro), Matteo Carlini (Arm), Dan Handley(Arm), Lionel D (ST), Andrej Butok (NXP), Julianus Larson (Linaro), Julius Werner (Google), Shebu Varghese Kuriakose(Arm), Kevin Townsend(Linaro), Don Harbin (Linaro), Eric Finco(ST), Michael Thomas (Renesas)

Minutes:

OP TEE Roadmap - Ilias provided overview

- Ilias: Eventually want Hafnium running with OP-TEE, with Xtest working
    - Ilias: According to Jens, there's some in-flight patches in Hafnium (from OlivierD) to make this work.
    - Matteo: Hafnium has been updated to FF-A 1.1. There may be some issues here
    - Ilias: Yes, that's the kind of thing that needs merging
    - Matteo: Just want to make sure he and Olivier are talking. Make sure they're aligned
    - Ilias: Yes, they're talking.
- Gyorgy: So this is the use case where OP-TEE is running as a S-EL1 SP, not as an SPMC?
    - Ilias: Correct
- Ilias continued walk thru of OP-TEE summary slide
- Ilias: Regarding crypto improvements, the Global Platform (GP) requirements have changed. SHA3 support is now mandatory
- Ilias: We want to start work to "access single OP-TEE instance from multiple VMs" after all TPM work is done
- Ilias: IBART is a test tool developed by OP-TEE team. We want to add support for new boards and new test functionality
- Ilias: We can now load TAs from different vendors with different (sub)keys
    - Ilias: This provides protection against Fault Injection (FI) attacks in TA loader.
    - Ilias: It might not be scaleable to implement this in the rest of the OP-TEE core.
- Lionel: Any follow up on "multiple signer support for vendors"?
    - Ilias: Not properly discussed but we're probably going to add it.
- Ilias: No driver support in OP-TEE for TPM
    - Ilias: Might be difficult to do
    - Ilias: Generally don't want full TPM drivers in secure world
    - Ilias: Verifying security of these is a huge effort
    - Ilias: But we do have some fundamental support there
    - Ilias: E.g. We have a supplicant that talks to RPMB. This has a rollback counter, and data storage (encryption is optional).
    - Ilas: TPM provides the same thing (and more). Can direct calls to either RPMB or TPM.
    - Dan: So you don't provide access to all the other TPM services that are hard to verify?
    - Ilias: Correct. We don't expect to implement a fTPM in OP-TEE
- Lionel: What is "Loading SP images from the TF-A FIP"?

    - Gyorgy: SP images were loaded in their own format.
    - Gyorgy: This support enables TF-A BL2 to load the SP from the same Firmware Image Package (FIP) containing OP-TEE and other firmware.
    - Gyorgy: OP-TEE still unpacks ELF image in SP.

EU Cyber Resilience Act: Kevin Oerton

- Kevin presented a webinar on the EU Cyber Resilience Act. Content to be attached to minutes.
- Presentation leads w/ Biz side, added implications to TF projects
- Kevin provided overview of the content
- Kevin: Thought it might be good to give some context of CRA and what it means for TF.org projects
- Kevin: Huge impact of Cybercrime - 3rd largest economy
- Kevin: Potentially huge disruption - loss of data, investigation costs, loss of reputation, …
- Kevin: In the context of an IoT product, the CRA covers both the physical product and any sw that works with it (e.g. cloud support sw and Android/IOS app).
- Kevin: A vulnerability in a product can affect the whole supply chain and may have catastrophic impacts including loss of life.
- Kevin: EU found 66 cases of using zero-day exploits.
- Kevin: There are a total of 85 in-depth requirements you have to comply with to get the CE mark.
- Kevin: As well as manufacturers, this affects also distributors/importers.
- Kevin: Could be prevented from selling the product or even be forced to recall them.
- Kevin Townsend : Can you provide the list of requirements?
    - Kevin O will provide to put in the minutes
- Kevin: After approval, you have 1 year to conform with vulnerability handling requirements, 2 years for full compliance
- Eric: Lifetime support refers to end products - any guidance on how this affects subsystems used to build the products (e.g. microcontrollers)?. Could mean we have to support products even longer.
    - Kevin: For a product to have a 5 year lifecycle, then along with that, need to disclose the top level s/w BOM.
    - Kevin: So if a product includes TF and an ST microcontroller and a vulnerability is found, then those dependencies must be ready to report to the OEMs.

- Kevin: Considerations for TF
- Kevin: After exploit, you have to notify ENISA and disclose to vulnerability database
- Dan: Is this EU vulnerability DB new? What about using Mitre CVEs instead?
    - Kevin: You have a reporting responsibility to ENISA but you can use other vulnerability DBs
    - Kevin: If a vulnerability is never actively exploited, there's no obligation to disclose publicly.
    - KevinT: The active exploit wording seems to be a loophole, but I will check the legislation.

    - KevinT: There seems to be a perverse disincentive to stick one's head in the sand and not see active exploits
- Dan: Actually Mbed TLS reports its vulnerabilities elsewhere (slide 13), but I agree this is very manual: https://mbed-tls.readthedocs.io/en/latest/tech-updates/security-advisories/
- Dan: Is there any active use or compulsion to use the standards in slide 14?
    - Kevin: Cisco and Redhat are exploiting these automation toolsets. Much of it is new, but already in use (example CSAF).
    - Kevin: I think it's important to get ahead of what's coming down the road soon.
    - Dan: Some of these look interesting (e.g. VEX). TF uses SPDX for licensing/copyright headers, but not for SW BOM
- **Post-meeting note from Kevin**: NXM is using the ENISA Good Practices as the proxy for the final EU CRA compliance requirements which have not yet been published.
    - https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT