TEEP requirements relevant to “Class ID” discussion

Dave Thaler <dthaler@microsoft.com>

Trusted Execution Environment Provisioning

- Quick summary:
  - SUIT manifest format is used to express dependencies and reference firmware/software updates and installation steps
  - TEEP is used for remediation when attestation fails due to a TEE being out of compliance
  - The TEEP protocol uses:
    - EAT for attestation
    - SUIT manifests for applying updates
  - EAT claims are then used to determine which SUIT manifests are applicable for remediating
- draft-ietf-teep-architecture lists TEEP requirements
  - WG state: Submitted to IESG for Publication

Requirement #1: Class of device

"The following information is required for TEEP attestation:
- Device Identifying Information: Attestation information may need to uniquely identify a device to the TAM. Unique device identification allows the TAM to provide services to the device, such as managing installed TAs, and providing subscriptions to services, and locating device-specific keying material to communicate with or authenticate the device. **In some use cases it may be sufficient to identify only the class of the device.** The security and privacy requirements regarding device identification will vary with the type of TA provisioned to the TEE."

- Possible examples:
  - A given SGX enclave library runs on any *SGX2 capable* Intel processor
    - (Narrower than manufacturer, broader than specific processor type/version/revision)
  - Same could be true of other processor features beyond TEE use cases
  - But manufacturer-specific means up to the manufacturer to define values/meanings

Requirement #2: Type of TEE

"- TEE Identifying Information: The **type of TEE** that generated this attestation must be identified. This includes version identification information for hardware, firmware, and software version of the TEE, as applicable by the TEE type. TEE manufacturer information for the TEE is required in order to disambiguate the **same TEE type created by different manufacturers** and address considerations around manufacturer provisioning, keying and support for the TEE."

Possible examples:

- OP-TEE runs on TrustZone on Arm Cortex-A processors from multiple manufacturers that all comply with a given spec/rev
- A trusted app runs on RISC-V TEEs from multiple manufacturers that all comply with a given spec/rev
- Non-TEE-specific: A given image runs on Arm Cortex-M processors from multiple manufacturers that all comply with a given spec/rev
- Here each value is associated with a given spec/rev, not manufacturer specific

Requirement #3: Software/firmware info

- “- TEE Identifying Information: The type of TEE that generated this attestation must be identified. This includes **version identification information for hardware, firmware, and software version of the TEE**, as applicable by the TEE type. TEE manufacturer information for the TEE is required in order to disambiguate the same TEE type created by different manufacturers and address considerations around manufacturer provisioning, keying and support for the TEE.”
- NOT (in my view) a “class ID”, a SWID/CoSWID seems sufficient here

Discussion