Scoping & Charter Discussion

Review of charter text

- <see charter text>

Software Update for Internet of Things (SUIT) BoF

- Was just held on Monday Nov. 13, 2017
- (Now obsolete) draft charter: https://datatracker.ietf.org/doc/charter-ietf-suit/
  - Proposed charter text being updated based on SUIT BoF outcome
  - SUIT BoF agreement that SUIT is not just for Class 1 devices, but a solution has to be implementable even on devices that are only Class 1 (~10 KiB RAM, ~100 KiB flash)

Relationship between TEEP and SUIT

In *currently* proposed charters (subject to change):

- TEEP focuses on more on trusted “apps” after boot, whereas SUIT focuses more on “firmware” for boot
- TEEP focuses on installation of code into a Trusted Execution Environment (whether for IoT or not), whereas SUIT focuses on installation of code on an IoT device (whether in a TEE or not)
- TEEP focuses more on initial provisioning of code the first time, whereas SUIT focuses more on subsequent updates to already-provisioned code

What SHOULD the work split be?

What changes should be made to the charter to reflect this relationship?

Relationship to GlobalPlatform

- July 2016: first individual I-D for OTrP (draft-pei-opentrustprotocol-00)
- 2016: GlobalPlatform passed on working on OTrP
- IETF 98 (March 2017): First TEEP non-WG-forming BoF
- IETF 99: Side meeting in July 2017, lots of attendees including draft authors, got agreement on problem scope and proposed charter
- But now GlobalPlatform apparently changed their mind…

GP folks notified IETF in October

- Jeremy (QC): “the contribution of OTrP to GlobalPlatform is a slightly later draft of draft-pei-opentrustprotocol-04.txt. I believe that any differences between the contributions at GlobalPlatform and IETF are only the result of differing contribution dates. Work has progressed at GlobalPlatform and there are now **significant clarifications and precisions in aspects of Security Domain behaviour and functionality** in internal drafts. … GlobalPlatform has chosen to restructure the OTrP contribution so that it fits better with the existing GlobalPlatform TEE specification structure.”
- Hank (GP): GlobalPlatform is creating an implementation independent specification including compliance test to verify interoperability of implementations. **The creation of an apparently similar specification in IETF will cause market fragmentation and interoperability challenges**.

GlobalPlatform process

- Jeremy (QC): The GlobalPlatform working groups are **open only to members**. Published specifications are free to download, but reside behind a “click-through” license. GlobalPlatform is open in the sense that anyone wishing to **pay the appropriate membership fee** can participate
- Hank (GP): GlobalPlatform specifications are open for public review before they are published. **During the public review period**, anyone can download and provide contributions to the specifications. The timeline from Public review of the GlobalPlatform OTrP specifications is expected to be **1Q 2018**.”

OTrP and Global Platform

- Global Platform (GP) defined a similar TEE Management Framework (TMF)
- OTrP was a different initiative, considered more lightweight and emphasized more on trust establishment
- GP only took OTrP from this August (08/2017) after IETF BoF progress
- GP created a mapping of OTrP JSON commands to TMF's ASN.1 commands
- TMF has more TEE state management functions that was out of scope of OTrP. It is an issue within GP itself.

Reasons raised ***for*** IETF doing OTrP:

- Non-technical reasons given by various people:
  - IETF is more open
  - IETF provides broader review during spec development
  - IETF culture promotes multiple interopable implementations, and early implementation
- Technical reasons:
  - David Wheeler: we have some issues with “too close” relationship to GP, because GP’s definition of TEE security ties that security to trusted boot … Too close a relationship to GP will create issues around this definition … by definition it rejects certain Intel TEEs (SGX primarily) and then Intel would consider this an implementation specific definition aligned to TrustZone, and *not a general TEE protocol*
  - Technical discussion on IETF list about transport protocol, encoding format(s), etc. may result in significant protocol changes or additions to be a general TEE protocol
  - Ability to reuse some common mechanisms between SUIT and TEEP

APIs

- The OTrP I-D specifies both a **protocol** and a **concrete API**.
- In general, IETF doesn't do concrete APIs (i.e., APIs in specific programming languages), just **abstract APIs**. Other orgs own concrete APIs, like W3C does JavaScript, the POSIX standard covers C, etc.
- GlobalPlatform does do concrete APIs for TEEs

Scoping Questions

- Should the IETF do work in this area?
- If yes, what should the *charter* say we/won't do (as opposed to just leaving decisions to the proposed WG)
    a) Transport protocol bindings (none in -04 draft)?
    b) Scaling down to constrained devices?
    c) …

Typical BoF Questions

- Is the problem sufficiently understood?
- Is the problem tractable?
  - This includes discussion of the correct scoping of "the problem" (too broad, too narrow, whatever)
- Is this the right place to address "the problem"?
- Who is willing to author specs?
- Who is willing to review specs?