IETF 100 TEEP BoF in Singapore
Wednesday, November 15, 2017
13:30-15:00 (+8) Collyer

Jabber: xmpp:teep@jabber.ietf.org?join
MeetEcho: http://www.meetecho.com/ietf100/teep

Agenda bashing, Logistics -- Chairs (5 min)

-no bashing

Problem statement -- Chairs (30 mins)
draft-liu-opentrustprotocol-usecase-01

Dave is presenting the problem statement on behalf of a group of individuals

Eric: Are applications running in a TEE isolated from each other?

Dave: Yes.

EKR: (etherpad crashed)

Dave: This effort is focused on the establishment of a TEE, and not the contents of the code running inside.

The slide "Entity Roles and Experience" was developed since the last BoF to make the problem more clear.

Q&A on the problem statement:

Eric: What happens when you run multiple applications in a TEE?

Dave: The TEE is issoating the applications from each other. Access to trusted peripherals is managed by the TEE

Hannes: There are a bucnh of different TE solutions that vary in capability. There are common attacks. We can solve some of this through standardization isolation.

Dave: A primary motivation is to get an app into a TEE, regardless of how many apps or TEEs you have.

Marc Blanchet: Does this entaoil software updates?

Dave: We will get to this later.

David Wheeler: A TEE should be able to attest to it's identitiy. Then you can figure out what characteristincs are available and decide if you want to allow an app to run in the TEE. This can be made by policy decision, which can consider other things like what is running in a TEE.

Dave: Good points. Is it important to allow a TEE to attest what it is?

???: Is the goal a standardized interface?
Dave: The goal is to define the protocol for #4 on "Entity Roles and Experience". The goal is provide a complete solution to this.
Sorin: It is important address different needs around what is attested to.
Henk: The most important thing to attest to is the identify of the TEE
Dave. That is one thing.
Henk. You also need to attest to the contents of the TEE.
Dave: Other groups have ways of doing this type of attestation., but this effort needs to support visibility into that.
Henk: Does the distinction between an attestation vs an appraisal of the attestation matter?
Dave: We need to work that out after we get chartered.
EKR: Is the approach to allow diffent implementation such as SQX and TrustZone, but allow the management to be the same?
Dave: Yes.

Review of proposed charter text -- Chairs (10 mins)
https://datatracker.ietf.org/doc/charter-ietf-teep/

Nancy is presenting. Reading the charter text.

???: I don't see the term audit in here? Will the workflow allow for verifying that some capabilities are in the TEE
Henk: Does that involve knowing if the contents of a TEE are new or old
Dave: We need to focus on understanding what should be in the charter, what should be clarified, and then we can do editing later.

Dave is covering the relationship to SUIT.

Is the work split right?
Hannes: The first axis makes sens, the other axis are secondary.
Marc: The lines are blured. What is firmware? What is boot? I am concerned thqat overlap will lead to divergence in solutions.
Henk:
Erik: I think we should have a single manifest that will work for both.
Kyle Rose: Adding to marc's point, the second bullet leaves out stuff that is addressed in normal ways. Seperate this out by

provision, trusted update, then what you want to run as a trusted app.
Hannes: We are not talking about booting in more capable devices. Simple booting using a small boot loader.
Carsten: Ask what it is and what . We need to be careful that what we design is not made unsutable for suit.
Spencer: Appreciates this discussion. Teep will run in more environments than suit?
Hannes: Smartphones run with trustzone, but IoT run a small code running directly on the hardware.
Spencer: It was not obvious that both SUIT and TEEP need to work on Class 1 devices. Perhaps a statement in the charter might help to claify this.
Dave: Summarizing, the charter should be more explicit about the types of machanisms used for provisioning. These machanisms might be differnt in TEEP from what might be used in a class 1 device. We will work with the IESG to find text that makes them happy.

Dave presneting slides on OTrP, GlobalPlatform, and IETF.

Joe Hildabrand: (as liason) We need to establish a liason if we do work on both sides
Carsten: We should avoid an apperance of bullying another SDO.
Kyle Rose: In the general case, the charter should be broader. Some apps may need capabilities that otherr may not. e.g, you can't use a virtual TPM in some apps. It would be nice to have a general framewwork. This may be well beyond the mandiate of the IETF.
Pete Resnik: clarifying that he does not know Jeremy well, while working at QC) Is there sme way to pull OTrP out of GlobalPlatform? We should wait on chartering until we sort out what the GP process will be.
Dave: Should we delay use case discssion since the IETF has a broader use cases than GP
Kathleen: ???
: We need interop

Hum: Is it useful for the IETF to do some work on this?
- Work on TEE provisioning? Strong consensus for yes, the IETF should do something. 80/20. some hummed that the question was not completely clear.

There is a question that we may want to slow down to better understand what otherr SDOs are doing.
Kathleen: We can get some of this with scoping. Doing work that is seperable.

Hum: Do you think that the core protocol overlapping with the GP work), should be in scope for the charter. Strongest was unclear.

Hum: Transport protocol bindings in scope. Strongest was yes.

Hum: Should we work on scaling down to constrained devices. Strong for yes.

Hum: Should an abstract API be in scope? Even across. Show of hands Yes=mostly in front of te room, but hands about equal from yes to I don't know.

Other questions:

Joe Hildabrand: Please email if you want to help on a laison.

Charter discussion   -- Chairs (45 mins)
