DRAFT

Confidential Computing Consortium

Minutes of the Meeting of the Technical Advisory Committee

23 January 2020

Members of the Technical Advisory Committee Participating in the Meeting:

- Mike Bursell (Red Hat)
- Grant Likely (Arm)
- Dave Thaler (Microsoft)
- Simon Johnson (Intel)
- John Haxby (Oracle)
- Zhipeng 'Howard' Huang (Huawei)

Not in attendance:

- Xiaoning Li (Alibaba)
- Gilad Golan (Google)

Guests and Observers:

- Richard Searle (Fortanix)
- Jethro Beekman (Fortanix)
- Seth Knox (Fortanix — Outreach Committee Chair)
- Faiyaz Shahpurwala (Fortanix)
- Stephen Walli (Microsoft. — GB chair & scribe)
- Simon Leet (Microsoft — OE SDK developer)
- Pushkar Chitnis (Microsoft — OE SDK developer)
- Omkhar Arasaratnam (JP Morgan Chase)
- Ahmad Atamlh (Mellanox)

Roll Call and Introductions: There was a roll call attendance, and brief introductions for new attendees.

Previous Minutes: The previous meeting minutes were discussed and unanimously approved. https://lists.confidentialcomputing.io/g/tac/files/Meetings/2020/CCC%20TAC%20Minutes%202020-01-16.pdf

RESOLVED: That the minutes of the Jan 16, 2020 meeting of the Technical Advisory Committee meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

DRAFT

Action Item Review:

1. Project Proposal Template has moved from wiki to Github to allow better collaboration.
2. Action on Simon and Jesse (Intel) about documents that the Consortium might publish as white papers to coordinate with the Outreach committee, has been moved to Seth (chair of Outreach) and Dave.
3. A summary of the confidential computing scope discussion to be forwarded to the governing board. Still open as discussion comes to closure. [Dave]
4. [Mike Bursell]: Begin an email discussion to the TAC outlining multiple axis along which the TAC (and governing board) can categorize and discuss the scoping and definitional discussion. [Done – see appendix slides]

"Confidential computing" definition & CCC scope:
Dave Thaler reviewed the discussions to date. See slides in Appendix.

Discussion:

- Software TEE discussion (slide VSM and QEMU in appendix)
    - A software TEE is an environment where some or all of the properties of a TEE are provided in software.
    - The base root of trust is in hardware.
    - The HW is assuring the protection.
    - SGX uses a lot of SW to provide features. TEEs are a combination of HW/SW. SW TEE w/out HW backing is essentially a dev tool.
    - Observation that we seem to be conflating debate of functionality with things we trust. For projects we host, they need to identify the things that are to be trusted. Would need guidance for users (and not so early as to be in the project template) and it would be learned in the project.
    - Prefers a broader discussion including SW (RISC-V example)
    - TEE needs to be HW-backed regardless of amount of SW in discussion.
    - A project should be able to describe it's TCB. Since it's relatively critical the project should be able to describe its initial assumptions at project proposal time.
- Haxby slide discussion (slide in appendix):
    - A HW design should be accepted into CCC
    - Our scope should include all the plumbing that enables HW TEE. We're looking for characteristics that describe the HW to enable SW.
- Dave as chair attempted consensus on whether the TAC is comfortable with a broader or narrower focus on 'confidential computing'. There were views in both directions (staying focused on HW TEE and SW to enable their use versus opening the discussion to include things that are privacy preserving like homomorphic encryption.)
- The point is to make a presentation to the governing board to vote.

DRAFT

Next Face-to-Face Meeting:

- Still on track for San Francisco, 27 Feb. coincident with RSA conference.
- Proposed order: Outreach, TAC, then GB

Budget:

- OE SDK has requested $100K for CI/CD.
- TAC has requested details back to the OE SDK project.

GitHub:

- Code of Conduct is posted.
- 2 issues filed – a reminder to all to begin to work on GitHub through issues and pull requests whenever possible rather than waiting for TAC meetings.
- Project Proposal Template and List are posted.

Closing Items:

- Mailing list are presently opened and will be so until we need to begin to moderate.
- TAC agreed TAC minutes to be public on the wiki.
- Proposals for Meetings – TAC agreed to try 2 hour meetings every 2 weeks.
- Jethro — requested opinions on a couple of examples of possible projects that Fortanix may bring forward.

Action Item

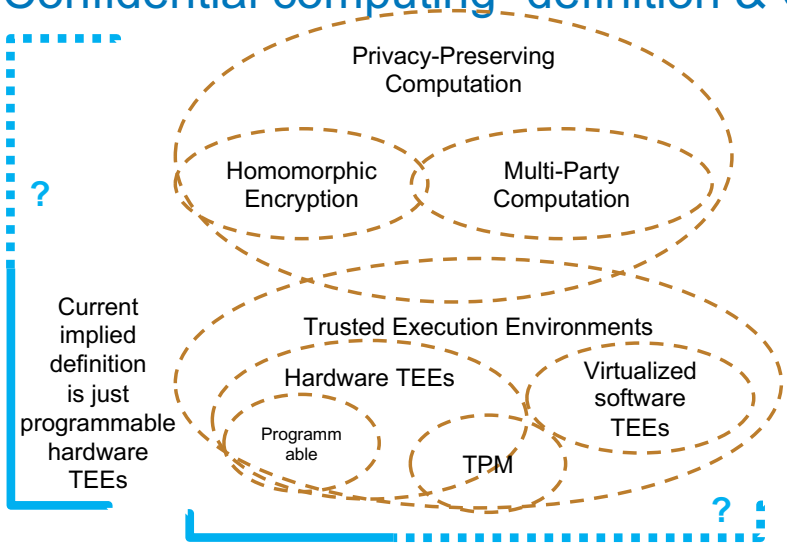
1. [Simon Johnson] Provide a proposal on project template changes for a project to describe its TCB.
2. [Pushkar Chitnis] Provide details for OE SDK ask on CI/CD pipeline costs.
3. [All] Review and comment on Code of Conduct on GitHub.

DRAFT

Appendix: Confidential Computing definition and CCC Scope

Summary slides presented and discussed.

"Confidential computing" definition & CCC scope



Disclaimer:
Some terms have multiple competing definitions, so boundaries are often fuzzy.

CONFIDENTIAL COMPUTING CONSORTIUM

Possible axes for categorising technologies

Rough consensus(?) that (at least) 5 axes make sense:

Axis	TAC Consensus?
algorithmic (mathematical) vs hardware/software	? (split opinions)
hardware (+firmware?) vs software	? (some argued for software too)
generalised vs specialised computation only	No one argued for non-programmable
on-main CPU vs off-main CPU	Broad?
cloud vs on-prem (incl. IoT)	Broad (whole axis)

Other attributes (e.g., TCB size) are also important evaluation criteria but by themselves weren't seen as part of scoping question per se

CONFIDENTIAL COMPUTING CONSORTIUM

DRAFT

Example technology	Hard-/software Implementation or Algorithmic	Hardware or Software)	Generalised compute or Specialised)	ON-main CPU (vs oFf-main CPU)	Cloud (vs on-Prem, incl. IoT)
Homomorphic encryption	A	---	S?	---	C/P
Multi-party Computation	A	---	G?	---	C/P
HSM	I	H	S (can be G?)	F	C/P
TPM	I	H	S	F	C/P
Hardware TEE on main CPU (e.g., SGX)	I	H	G	N	C/P
Virtualised software TEE	I	S	G	**N**	**C/P**
FPGA	I	H	S	F	C/P
TEE in NIC	I	H	S	F	C/P
Secure Element	I	H	S?	F	P
…?					

Additional external definition mentioned last meeting

- **Dedicated Security Component:** the combination of a **hardware** component and its controlling firmware dedicated to providing the encompassing platform with services for the provisioning, protection, and use of Security Data Objects (SDOs) consisting of keys, identities, attributes, and other types of Security Data Elements (SDEs).

  From https://www.commoncriteriaportal.org/communities/docs/cpp_dsc_v10d_DRAFT_20190501.docx

DRAFT

Software TEE examples

- **Virtual Secure Mode (VSM):** a software-based TEE that's implemented by Hyper-V in Windows 10 and Windows Server 2016. Hyper-V prevents administrator code running on the computer or server, as well as local administrators and cloud service administrators from viewing the contents of the VSM enclave or modifying its execution.
  - https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/
- **QEMU ("quick emulator"):** very widely used open source machine emulator. … Developers can use the QEMU Arm Security Extensions to develop and work with Trusted Execution Environments (TEEs) that are likely to be the primary consumers of the added functionality. Secure applications can then be developed on the added TEEs without the need for dedicated hardware.
  - https://www.linaro.org/blog/arm-trustzone-qemu/

CONFIDENTIAL COMPUTING CONSORTIUM

John Haxby wrote:

- After last week's meeting I think we almost had a definition of the scope as simple as
  - **"Software solutions to enable the widespread use of hardware trusted execution environments"**.
- "Software solutions" probably needs to be replaced by something else, perhaps even just "software" and perhaps "hardware" could be "hardware-assisted".
- So, clearly, all three projects adopted so far fall under that definition but some others might be useful:
  - A software TEE emulation for development
  - A virtual machine TEE using encrypted memory so no one, not even the hypervisor, can look inside it. (That would be "hardware-assisted perhaps".)
- A TEE in/on a NIC, GPU, discrete (socketed) chip, thumbdrive, etc all fall into the "hardware" category as something you physically hold.
- A TEE that relies on, for example, isolated or encrypted memory to keep its function away from prying eyes would be "hardware assisted". (SGX falls into that category doesn't it?)

CONFIDENTIAL COMPUTING CONSORTIUM