Technical Advisory Council (TAC) Meeting

October 15, 2020

CONFIDENTIAL COMPUTING CONSORTIUM

The Confidential Computing Consortium

A community focused on open source licensed projects securing DATA IN USE
& accelerating the adoption of confidential computing through open collaboration

Every member is welcome; every project meeting our criteria is welcome.
We are a transparent, collaborative community.

We as members, contributors, and leaders pledge to make participation
in our community a harassment-free experience for everyone.

Antitrust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Agenda

1. Welcome, Roll call
2. Approval of minutes
3. Action item review
4. CCC & CNCF SIG-Security
5. Interoperability project/SIG
6. TAC whitepaper
7. Areas of CCC Focus for Year #2
8. Any outstanding GitHub issues / pull requests (time permitting)
9. Any other business

Roll Call of TAC Voting Representatives

Quorum requires **5** or more voting reps:

Member	**Representative**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Ant Group	Zongmin Gu	zongmin.gzm@antgroup.com
ARM	Grant Likely / Michael	grant.likely@arm.com
Facebook	Jinsong Yu / Shankaran	jinsongyu@fb.com
Google	Brandon Baker	bsb@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Simon Johnson	simon.p.johnson@intel.com
Microsoft	Dave Thaler(*)	dthaler@microsoft.com
Red Hat/IBM	Mike Bursell / Dimitrios	mbursell@redhat.com

**TAC chair*

2. Approval of TAC Minutes from Sept. 17 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2020/09-Sept/CCC%20TAC%20Minutes%202020-09-17.pdf

RESOLVED: That the minutes of the September 17, 2020 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

Approval of TAC Minutes from Oct. 1 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2020/10-Oct/CCC%20TAC%20Minutes%202020-10-01.pdf

RESOLVED: That the minutes of the October 1, 2020 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

3. Action Item Review

1. [Mike] Ensure that a TAC budget line item for 1 Zoom account for OE SDK
2. [David Kohlbrenner/Stephano to remind] Please provide a list of the licenses used by Keystone for crypto implementations, specifically to ensure that they are all OSI approved.
3. [Stephano] Ping Mike if we can’t redirect Enarx mailing list
4. [Stephano] Work with the Occlum folks to get a list of the dependencies listed which are part of the TCB and add that to the submission document for posterity
5. [Aeva/Mike] Create straw-person for terminology proposal
6. ~~[Dave] Update the Project Progression Policy to match the board charter change regarding Graduation stage projects and voting [DONE]~~
7. [Stephen] Please reach out to Cat Allman regarding any details we can get on LISA21
8. [Stephano] Get the timing diagram graphic to LF Creative so that we can review it
9. [Stephano] Set up a vote for a chat system, pinging the LF to ensure that Slack is still the default / most popular choice

(TACWhitepaper-specific Action Items listed on later slide)

CONFIDENTIAL COMPUTING CONSORTIUM

4. CCC & CNCF SIG-Security - Aeva

5. Interop Working Group Proposal (Gilad Golan)

- Investigate and promote industry standards for:
    - Authentication of CC environments (attestation)
    - Secure communication with and among CC environments
    - Secure sealing of secrets to CC environments
- Proposal: Interoperability Working Groups or SIGs

6. TAC Whitepaper

- https://docs.google.com/document/d/17PhrIXvFJsAIJryYjpezmfdSI1BSB1x1tE2FTbriHyc/edit?ts=5ec71ac7
    - [Thomas] You suggested adding a sentence in the Introduction section about the intended audience, perhaps simply changing the last sentence. Any guidance here appreciated. This action item is a reminder to follow up on this in the next meeting.
    - [Mike] Please clarify the section 6.2.1 “Threat Vectors -> In-Scope” regarding crypto in hardware vs crypto in firmware/software.
    - [Michael] Please have an Arm attestation lead review the document before October 15

7. Areas of CCC Focus for Year #2

1. Cross-project coordination/communication
   - Cross-project chat (e.g., attestation channel)

2. Cross-org coordination
   - Standards orgs (IETF, GlobalPlatform, TCG, FIDO, HomomorphicEncryption.org, ...)
   - Government agencies (NIST, BSI, ...)
   - Open source orgs (CNCF, TrustedFirmware.org, …)

3. Additional collateral (whitepaper, terminology, talks)

4. Demos and tech talks in TAC meetings

8. Github PR’s and issues (time permitting)

https://github.com/confidential-computing/governance/pulls

- PR #62 (Update scoping doc from phrased as a future proposal to being phrased as statement of current state)
- PR #66 (Remove project specific votes in the TAC)
  - “Time bomb” label expires October 21

https://github.com/confidential-computing/governance/issues

- PR #50 (Define what a growth plan entails)

9. Any other business