Technical Advisory Council (TAC) Meeting

February 10, 2022

CONFIDENTIAL COMPUTING CONSORTIUM

This meeting is being recorded.

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.

CONFIDENTIAL COMPUTING CONSORTIUM

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.

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

1. Welcome, Roll call, Introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. TAC tech talk: Confidential Computing Mentorship - Nick
5. Code of Conduct escalation paths - Dan
6. Process improvement suggestions - Brian
7. Code scanning process
8. Updates from Outreach Committee
9. Common Terminology
10. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call, and Introductions

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	Thomas Fossati / Michael	thomas.fossati@arm.com
Facebook	Eric Northup / Shankaran	digitaleric@fb.com
Google	Iulia Ion	iuliaion@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton / Simon	dan.middleton@intel.com
Microsoft	Dave Thaler(*)	dthaler@microsoft.com
Red Hat/IBM	Lily Sturmann / Dimitrios	lsturman@redhat.com

**TAC chair*

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/12-Dec/TAC%20Minutes%202021-16-12.pdf

RESOLVED:
That the minutes of the Dec. 16, 2021 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.

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2022/01-Jan/CCC_TAC_Minutes-2022-01-27.pdf

RESOLVED:
That the minutes of the Jan. 27, 2022 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.

CONFIDENTIAL COMPUTING CONSORTIUM

Action Item Review

1. **[Mike, Eric V, Stephen, Zongmin]** Recommend diversity and inclusion training to their projects and report back to the TAC on whether the maintainers or the contributors will be taking it and when the expected completion date is.
    - Open Enclave maintainers are close to 100% trained (Dave Thaler)
    - Veracruz lead has taken the course (Thomas Fossati).
    - Please report back that project maintainers have been made aware of the training, and have been asked to take it.
2. **[Brian]** Share process for Linux Foundation license scanning with Keystone project.
    - Brian to follow up.
3. **[Thomas F., Mike B.]** Attestation SIG co-chairs to discuss / clarify goals.
4. **[Eric Voit]** Diagram and description on slide 3 of common terminology presentation to be added to the whitepaper draft.**[DONE]**
5. **[Dave]** Schedule Open Enclave annual review. **[DONE]**
6. **[ALL]** Review, comment and/or correct text in Common Terminology Document. **[ON AGENDA LATER]**

Project	Proposed by	TAC Approved	Tech. Charter	IP Assigned	Board Presentation	Board Approved	Annual Review	Mentor	Webinar
Enarx	Red Hat	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	14 JAN 2021	Mike Bursell	JAN 2021
OE SDK	Microsoft	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	12 NOV 2020	Dave Thaler	MAR 2021
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	1 DEC 2021	15 SEP 2021	4 NOV 2021	Eric V	(10 FEB 2022?)
Keystone	UC Berkeley	23 JUL 2020	Yes	Yes	24 JUN 2021	MAR 2021	13 JAN 2022	Stephen	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	15 SEP 2021	2 DEC 2021	Zongmin	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021	18 NOV 2021	Thomas F	APR 2021
CCC-Attestation	TAC	Yes	Yes	N/A	18 MAR 2021	18 MAR 2021		Dan & Aeva	
Veraison	Arm	4 FEB 2022						Howard	NOV 2021

CONFIDENTIAL COMPUTING CONSORTIUM

TAC tech talk: Confidential Computing Mentorship

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2022/01-Jan/TAC_Minutes-2022-01-13.docx

RESOLVED:
That the minutes of the Jan. 13, 2022 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.

CONFIDENTIAL COMPUTING CONSORTIUM

Code of Conduct escalation paths - Dan

Best practice is to have a clear reporting path, to a set of named individuals, which is published within the community

- For escalations.
- Documented recusal process, for situations where there may be a COI for someone on the panel.
- For accountability.

LF Projects and LF Events have a default escalation path

- For LF Projects, Mike Dolan as Series Manager.
- Escalation path and CoC can be overridden by projects establishing their own policies.

Proposal:

- Evaluate whether the default CCC escalation paths are sufficient, and draft an alternative if not.
- Determine whether projects need their own escalation policy, or they should use the CCC escalation policy.
- Add requirement that projects link to the escalation policy.

Process improvement suggestions - Brian

Move meeting materials to GitHub to improve discoverability

- “TAC” subdirectory in governance repo (https://github.com/confidential-computing/governance)
- Leave copy of existing files at groups.io so links don’t break.
- Meeting materials can be PR’d in (speaker presentations, etc.).
- https://github.com/confidential-computing/governance/pull/88

Record meeting minutes as markdown files

- Draft minutes would be PR’d into the repo.
- TAC members can review and make suggestions directly.
- When a vote passes approving the minutes, the PR can be merged.
- Trivial changes (spelling, formatting) can be merged directly.

CONFIDENTIAL COMPUTING CONSORTIUM

Process improvement suggestions

Use GitHub to store core project lifecycle docs

- A single location to store project applications, charters, links, and any other relevant information.
- Projects shouldn't need to store their own lifecycle documents, but the TAC and projects should always be able to find them.
- https://github.com/confidential-computing/governance/pull/90

Use YouTube to store meeting recordings (private, unlisted, or public)

- Cannot directly organize Zoom recordings into folders or playlists.
- Can create YouTube playlists (private, unlisted, or public).
- Can be streamed directly from the meeting to the YouTube account.

CONFIDENTIAL COMPUTING CONSORTIUM

Process improvement suggestions

Policy doc consolidation

- The governance repo has a number of separate policy docs.
- Should we make some updates to make things easier to find?
- For example:
  - Consolidate TAC process documents in one directory?
  - Maybe even a single authoritative file like `TAC/README.md`?

Code Scanning from the LF - Brian

Recap:

- **Intake Scan:** High level scan with an emphasis on finding all open source licenses present in the codebase, and some third party dependencies. We provide a summary report listing the licenses found, including any copyleft licenses and potential license conflicts. We do NOT examine every match to a potential license, and we do NOT provide a detailed file inventory showing where the license matches occur. In order to do any follow up or recurring scans, a full baseline scan will be necessary first.

- **Baseline Scan:** Full scan, where every license match is examined. A detailed report is provided including a complete file inventory for every license match, and detailed findings for any copyleft license or other potential license issues found. This can potentially take significantly longer than an intake scan, depending on the size of the codebase. The baseline scan results are stored and are available for doing incremental / recurring periodic scans.

Scanning

Completed FOSSology scans (as of Sept. 16)

- Open Enclave SDK
- Enarx

Process for initiating a scan and getting access to results:

- Please ask an LF staffer, who will work with Legal to schedule the scan and distribute the results to core project participants.

Updates from Outreach Committee

- Ravi Sharma is the new Outreach chair, Nick Vidal is Vice-Chair.
- Gramine webinar rescheduled to 11am PST.
- Working on revising core priorities until Ashley’s replacement is in place.
- End User Advisory Council is planning two events.

Establishing common terminology (issue #79)

Github Issue:

- https://github.com/confidential-computing/governance/issues/79

Doc in progress:

- https://docs.google.com/document/d/1xZ6IX0w0jaWDbLMFNAybTF3FpLnQ5TJ98nzIWbsbFnY/edit#

Anjuna glossary slides from last meeting:

- https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/11-Nov/AnjunaDefinitions.pdf

CONFIDENTIAL COMPUTING CONSORTIUM

Any other business

Date	CCC Project Review	TAC Tech Talk
24 FEB 2022	Open Enclave SDK annual review	TCG work on Confidential Computing - Henk
10 MAR 2022		
24 MAR 2022		
5 APR 2022		Confidential computing from the perspective of the network – Penglin & Eric V.

CONFIDENTIAL COMPUTING CONSORTIUM

List of suggested future topics

- Rust Hypervisor firmware: https://github.com/cloud-hypervisor/rust-hypervisor-firmware - Dan to provide contact
- IETF Trusted Execution Environment Provisioning (TEEP) work – Dave
- Logging and error reporting in confidential computing – Mike B.
- Confidential computing from the perspective of the network – Penglin & Eric V.
- DARPA Data Protection in Open Environments (DPRIVE) – Dan contacted

Reference: CCC project benefits

CCC projects have access to a number of benefits:

- Up to $7,500 in budget for hardware and software per year.
- Funding for one Outreachy intern.
- TAC mentor assigned to the project.
- Collaboration tools (contact operations@confidentialcomputing.io):
  - Zoom
  - Domain registration and renewals
  - Mailing lists
  - YouTube playlists
- Optional security scanning
- LFX tools (https://lfx.linuxfoundation.org).

CONFIDENTIAL COMPUTING CONSORTIUM

Reference: CCC project expectations

CCC projects are expected to:

- Participate actively in CCC activities (webinars, newsletters, events, etc.).
- Notify the TAC and Outreach committees of relevant news.
- Participate in an annual review with the TAC.
- Inform the TAC when dependencies change so records can be updated.
- Maintainers should take the Linux Foundation's free Inclusive Open Source Community Orientation training course.
- Transfer trademarks and domain registrations to the Linux Foundation

CONFIDENTIAL COMPUTING CONSORTIUM