Technical Advisory Council (TAC) Meeting

November 18, 2021

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, Introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. Updates from Outreach committee
5. TAC Tech Talk schedule
6. **Annual Project Review: Veracruz**
7. Budget Planning status
8. Common Terminology
9. Any other business

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*

2. Approval of TAC Minutes from Nov. 4 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/11-Nov/TAC%20Minutes%202021-04-11.pdf

RESOLVED: That the minutes of the Nov. 4, 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.

3. Action Item Review

1. [Ashley] Reach out to project mentors to confirm potential security contacts for each current and upcoming project
2. [Project Mentors] Recommend diversity and inclusion trainings 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
3. [Ashley] Seek clarity on the process for recommending projects to participate in industry events. Should the outreach suggest this or are project mentors responsible for notifying their projects?
4. [Dave] Coordinate with organizer from LPC microconference about linux-collab list.
5. [Ashley/Brian] Gather documents to create spreadsheet for CCC security reports and VMT process.
6. [VMT Subteam] Meet with Stephen to identify the process for establishing VMT.
7. [Ashley] Notify Keystone of their project review on December 16th [DONE, moved to Jan 13]

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
SGX SDK for Linux	Intel	31 OCT 2019			31 OCT 2019			(Simon Johnson)	
TCF	Intel	28 MAY 2020							
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	(Nov 2021?)	15 SEP 2021	4 NOV 2021	Eric V	FEB 2021 (DEC 2021?)
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	(4 DEC 2021?)	Zongmin	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021	18 NOV 2021	Grant & Mike	APR 2021
CCC-Attestation	TAC	Yes	Yes	N/A	18 MAR 2021	18 MAR 2021		Dan & Aeva	(Veraison – NOV 18?)

4. Updates from Outreach Committee

7. TAC Tech Talk schedule

Invited:

- RISC-V Consortium – Jeff Scheel / Mark … (currently scheduled for Dec. 2)
- TCG POV on CC – Henk Birkholz (invited, date TBD)
- OP-TEE from TrustedFirmware.org (Thomas Fossati to invite)
- Homomorphic Encryption + Confidential Computing – suggested by Outreach (Dave contacted)
- Veraison? – was presented in CCC-Attestation, and webinar today, but not to TAC
- Results of Outreachy program – Nick
- 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.
- One 30-min talk per meeting? Can we do an annual project review + a TAC Tech Talk + other

6. Annual project review: Veracruz

CONFIDENTIAL COMPUTING CONSORTIUM

5. 2022 Budget Planning

- Two test infrastructure proposals discussed last meeting:
  - PROPOSAL 1: The TAC may provide up to $7,500 towards hardware (incl. cloud hosting time on TEE services) per annum per project on request by the project and approval of the TAC.
    - [ ] Yes [ ] No
  - PROPOSAL 2: The TAC may provide up to $15,000 of hardware per annum on TEE test infrastructure that is usable by multiple projects.
    - [ ] Yes [ ] No
- Could be used for CAPEX or OPEX

2022 Budget Planning

- Reminder of TAC Resources available to projects on request:
    - LF License Scanning
    - Slack instance
    - Groups.io email list hosting
    - Outreachy intern: $6500/yr per qualifying project
    - Test infrastructure: $15000/yr common, $7500/yr per qualifying project
    - Zoom account
    - **LF Creative, e.g. logo creation: $?**

5. 2022 Budget Planning status

Description	2021 Budget	2021 Jan-Aug	2021 Forecast	2022 Budget	Notes
LF License Scanning	$10,000	$6,000	$10,000	$12,000	
IT Services and Collab tools	$5,700	$3,352	$3,864	$3,864	website, groups.io, paid Slack
Hosting and other costs	$0	$0	$10,000	$10,000	Used if someone needs a software license or something else simple
Consortium IT Services and Collab Tools	$270,000	$0	$50,000	$100,000	Budget for use by projects
Common test infrastructure	N/A	N/A	N/A	$15,000	
Project test infrastructure	N/A	N/A	N/A	$60,000	Up to $7500 per qualifying project
Outreachy interns	N/A (Outreach)	N/A (Outreach)	N/A (Outreach)	$52,000	$6500 per qualifying project
TOTAL	**$285,700**	**$9,352**	**$73,864**	**$252,864**	

8. 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

9. Any other business

Reminder: annual chair election

- TUE Nov 3, 2021: Call for nominations opens
- TUE Nov 10, 2021: Call for nominations closes
- WED Nov 11, 2021: Voting period opens
- **WED Nov 18, 2021: Voting period closes**
- TUE Nov 24, 2021: Election results announced