Technical Advisory Council (TAC) Meeting

August 11, 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.

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

   Welcome new Google representatives

2. Approval of minutes
3. Action item review
4. Tech Talk: MPC + TEE (30 mins) - Jordan Brandt?
5. Governance SIG Charter (15 mins)
   a. SIG charter document (2-3 pages) defining our goals
   b. The very early thinking around how we'll be developing and standardizing reusable patterns around governance
6. Finalize Common Terminology whitepaper for LF CS
7. TEEP-Usecase-for-Confidential-Computing-in-network in IETF 114 TEEP (2 mins)
8. Testing

   Enarx hardware email - Vote to increase hardware budget to 10k

   Common Test Infrastructure

9. Updates from Outreach committee
10. Review of open pull requests/issues (time permitting)
11. Any other business

Roll Call, and Introductions of new attendees

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

Member	**Representative / Alternate**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Ant Group	Hongliang Tian (Tate)	tate.thl@antgroup.com
Arm	Thomas Fossati / Michael	thomas.fossati@arm.com
Facebook	Eric Northup / Shankaran	digitaleric@fb.com
Google	Cfir Cohen / Catalin Sandu	cfir@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://github.com/confidential-computing/governance/pull/124

Proposed:

That the minutes of the July 14, 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.

Action Item Review

1. [Stephen] 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. (Please report back that project maintainers have been made aware of the training, and have been asked to take it.)
2. [Mentors] Mentors to reach out to the project for getting the maintainers involved in Common Test Infrastructure
3. [Kurt/Helen] work with Outreach for setting up a first draft of the CCC wikipedia page - (Outreach agenda item)
4. [Mark N, Thomas F, Naveen C, Steve VL, Eric N] governance subgroup - collaborating on the governance topic, SIG formation and status update requested
5. [Mentors] Code scanning via LFX Security - add all missing projects to security for scanning, get more details on instructions on installing GitHub bot
   - Projects can set up the bot and repos they want scanned by following these instructions: https://community.lfx.dev/t/how-to-install-and-configure-bots-to-secure-your-projects/181
6. [KT] to set up a meeting to define scope and technical requirements with LF IT, Dave T, Dan M, Alec F, Nick V (LF IT ready) - Test Infrastructure
7. [Mentors/Kurt] to collect questions for determining interest in creating an "Infrastructure" slack channel for discussing best practices by July 28th meeting, Kurt to send a reminder mail July 21st
8. [Eric V] Requested to post common terminology diagram source
9. ~~[Mark N, Eric V and Alec F] - Send email to EUAC to assist in definition of marketing terminology (Done)~~
10. ~~[Kurt] Add budget slide to next meeting agenda (Done)~~

TAC Tech Talk

- MPC + TEE
  - Jordan Brandt - MPC Alliance

Governance SIG proposal

- Proposed SIG charter
- Early thinking around governance patterns

Establishing common terminology - Whitepaper

Doc in progress:

- First draft committed to github, revisions will be handled as PRs
- https://github.com/confidential-computing/governance/blob/main/terminology/common-terminology.md
- LF Creative Services engaged for document conversion and formatting for whitepaper PDF
- First Draft completed and under review
- Needs to be finalized for last updates to LF CS

TAC Review - Common Terminology White Paper

See white paper draft in governance/terminology

https://github.com/confidential-computing/governance/issues/116

https://github.com/confidential-computing/governance/issues/117

- Feedback from Microsoft Azure folks [Ananya & Alec]

Budget as of 6/30/2022

	2022 Approved Budget	YTD Actuals thru June 22	June 2022	Remainder	Notes
License Scanning	$12,000	$0	$0	$12,000	
Test infrastructure	$75,000	$0	$0	$75,000	Common $15k, Project $60k
IT Services and Collab Tools	$3,864	$4,233	$758	-$369	
Non-Capital Equipment			$0	-$4,961	Custom Exxact Workstation & Amazon order (Gramine)
Community Support	$0	$0	$0	$0	
Consortium IT Services and Collab Tools	$100,000	$0	$0	$100,000	
Hosting and other costs	$10,000		$0	$10,000	
Internships	$52,000		$0	$52,000	Outreachy

Enarx hardware email

Vote to increase hardware budget to 10k

Common Test Infrastructure

- Needing to meet with LF IT for sizing and technical requirements
- Approved: 50K for infrastructure management and 15K for hardware
- Would any project use such infrastructure if it existed?

Updates from Outreach Committee

- August webinar topics/candidates?
- Wikipedia Confidential Computing Consortium page
  - Outreach will use the first whitepaper as a template and TAC will
  - Currently redirects to LF page
  - https://en.wikipedia.org/w/index.php?title=Confidential_Computing_Consortium&redirect=no
- https://en.wikipedia.org/wiki/Trusted_execution_environment

Reference: past TAC tech talk topics

- 2021-10-07: Kata containers
- 2021-10-21: Protecting critical infrastructure
- 2021-12-02: RISC-V security overview
- 2022-01-13: Homomorphic Encryption
- 2022-01-27: OP-TEE and Trusted Services
- 2022-02-10: Confidential computing mentorship
- 2022-03-10: Overview of TCG confidential computing
- 2022-04-07: Governance
- 2022-05-05: IETF Trusted Execution Environment Provisioning
- 2022-05-19: Logging and error reporting in confidential computing
- 2022-06-02: Multi-TEE systems: PCI-SIG WG
- 2022-06-30: Blueprints for Enclaves

Time permitting: Review of open issues and PRs

Current open issues in the Governance repo:

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

Current open PRs in the Governance repo:

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

Any other business / Schedule

Date	CCC Project Review	TAC Tech Talk
11 AUG 2022	(governance)	
25 AUG 2022		
15 SEPT 2022		MPC + TEE
22 SEPT 2022		NSF Center for Distributed Confidential Computing. Prof Xiaofeng Wang

Tentative TAC talk topics

- Rust Hypervisor firmware: https://github.com/cloud-hypervisor/rust-hypervisor-firmware - Dan to provide contact
- Trust domains - Mike?
- Defined-Trust Transport (DeftT) Protocol for Limited Domains - Kathleen Nichols, Van Jacobson, Randy King
- NSF Award Search: Award # 2207231 - Collaborative Proposal: SaTC: Frontiers: Center for Distributed Confidential Computing (CDCC) - (Mona highlighted this)

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	10 MAR 2022	Nick Vidal	JAN 2021
OE SDK	Microsoft	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	24 FEB 2022	Dave Thaler	MAR 2021
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	1 DEC 2021	15 SEP 2021	4 NOV 2021	Eric V	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-Attest ation	TAC	Yes	Yes	N/A	18 MAR 2021	18 MAR 2021	21 APR 2022	Dan & Aeva	21 JUNE 2022
Veraison	Arm	4 FEB 2022	Yes	Yes	16 MAR 2022	18 May 2022		Howard Huang	NOV 2021

Deferred topics

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

Code Scanning from the LF

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.

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).