Technical Advisory Council (TAC) Meeting

June 30, 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. Draft - TAC response to the OSTP - Privacy-Enhancing Technologies
5. TAC Tech Talk - Blueprints for Enclaves
6. Finalize Common Terminology whitepaper for LF CS
7. Updates from Outreach committee
8. Common Test Infrastructure (time permitting)
9. Review of open pull requests/issues (time permitting)
10. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call, and Introductions of new attendees

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

Member	**Representative**	**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	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://github.com/confidential-computing/governance/pull/120

Proposed:

That the minutes of the June 16, 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. [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. [Thomas F] Update GitHub with Veraison charter (Done, in Veraison/community repo) - DONE
4. [Mike Bursell] Wikipedia update needed - Trusted Computing wiki page (Done)
5. [Kurt/Helen] work with Outreach for setting up a first draft of the CCC wikipedia page - (Outreach agenda item)
6. [Mark N, Thomas F, Naveen C, Steve VL, Eric N] governance subgroup - collaborating on the governance topic, SIG formation and status update requested at June 30 meeting
7. [Mentors/Kurt] Code scanning via LFX Security - add all missing projects to security for scanning, get more details on instructions on installing GitHub bot (Done - 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)
8. [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)
9. [Mentors] to collect questions for determining interest in creating an "Infrastructure" slack channel for discussing best practices

TAC response to the OSTP - Privacy-Enhancing Technologies

https://www.nitrd.gov/request-for-information-on-advancing-privacy-enhancing-technologies/

https://docs.google.com/document/d/1WdOGu2ZPpoIfpcQW7Vs_HCXM14X8CLuAcc4h_j5o4tw/edit

Review/approve draft response from Mike Bursell's email June 17th

Summary of topics for comment:

1. *Specific research opportunities to advance PETs*
2. *Specific technical aspects or limitations of PETs*
3. *Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs*
4. *Specific regulations or authorities that could be used, modified, or introduced to advance PETs*
5. *Specific laws that could be used, modified, or introduced to advance PETs*
6. *Specific mechanisms, not covered above, that could be used, modified, or introduced to advance PETs*
7. *Risks related to PETs adoption*
8. *Existing best practices that are helpful for PETs adoption*
9. *Existing barriers, not covered above, to PETs adoption*
10. *Other information that is relevant to the adoption of PETs*

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Tech Talk

- Blueprints for Enclaves - Paul and Eustace

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
- **TEEP Usecase for confidential computing in network - email from Penglin Yang**

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Review - Common Terminology White Paper

See white paper draft in governance/terminology

Updates from Outreach Committee

- July 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

Common Test Infrastructure

- Needing to meet with LF IT for sizing and technical requirements
- Approved: 50K for infrastructure management and 15K for hardware

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

CONFIDENTIAL COMPUTING CONSORTIUM

Any other business / Schedule

Date	CCC Project Review	TAC Tech Talk
2 JUNE 2022		Multi-TEE systems: PCI-SIG WG - Mark Novak
16 JUN 2022		
30 JUN 2022		Blueprints for enclaves
14 JUL 2022	(governance)	(trust domains?)

Tentative TAC talk topics

- Rust Hypervisor firmware: https://github.com/cloud-hypervisor/rust-hypervisor-firmware - Dan to provide contact
- Trust domains - Mike?

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	Mike Bursell	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-Attestation	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

CONFIDENTIAL COMPUTING CONSORTIUM

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

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).

CONFIDENTIAL COMPUTING CONSORTIUM