Technical Advisory Council (TAC) Meeting

December 15, 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

Etherpad - Meeting Minutes

- https://etherpad.lfnetworking.org/p/CCC-TAC-Minutes-2022-12-15

- Join the etherpad and set up your name and text color
  - Meeting attendance - please **add yourself**
  - **Voting Attendees just need to put a “+” next to their name**

- **Please** help make the meeting minutes be more accurate

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. 2022 Accomplishments
5. 2023 Goals
    a. Project Growth
6. Confidential Computing Summit - Raluca Popa
7. Conformance to terminology - Dave Thaler?
8. Outreach Update
9. Formalization for GRC SIG? (board, list in project matrix with mentor, ?)
10. Github Issue Cleanup
    a. Issue per TAC member
11. Any other business

Roll Call

Quorum requires **4** or more voting reps:

* *TAC chair*

Member	**Representative / Alternate**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Arm	Thomas Fossati / Michael	thomas.fossati@arm.com
Meta Platforms	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	Lily Sturmann / Dimitrios	lsturman@redhat.com

Introduction of new attendees?

Approval of TAC Minutes

https://github.com/confidential-computing/governance/pull/149

Proposed:
That the minutes of the December 1, 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. [Tate/Dan] Mentors to reach out to the project for getting the maintainers involved in Common Test Infrastructure
    - Update 12/15: Occlum prefers per project cloud budget rather than common infrastructure.(Per Tate) (DONE)
2. [Kurt] to verify that project messaging services are listed on the new website, something similar to eBPF Foundation projects summary
3. [Kurt] gather information on the job role for a Technical Architect role (In progress, Documenting responsibilities)
    - Update 12/15: First draft of role criteria
4. [Kurt] follow up with CDCC investigator for future tech talks
5. [Kurt] to direct the LF Creative to update revision date and version number for the TAC and Outreach whitepapers to reflect the definition change
    - Update 12/15: <wip as of 12/9 thanks, Helen>
    - Update 12/15: IETF RATS blocked on CCC updating our version and date.
6. [Ben Fischer] to follow up with the Outreach committee for review of both whitepapers
    - Update 12/15: Clarify has Ben accepted this Action Item?
    - Was the review targeted at capitalization of Confidential Computing? ← Yes
7. [TBD] New 12/15: Direct LF Creative to export the TAC whitepaper to markdown so we can put it under source control in our repo.

2022 Accomplishments

https://docs.google.com/document/d/1S6Ytq0Ie0ZZegMG2rJQOrlW6UjrLO-4OVkPwqAg03c8/edit?usp=sharing

Governance, Risk & Compliance SIG

- SIG created, charter agreed
- Membership includes a broad cross-section of industry participants
- Established a working relationship with CSA, joint WG starting soon
- Connected with NIST, expect to work together starting January ‘23
- Responded to the ICO request for comments around use of CC for privacy

CONFIDENTIAL COMPUTING CONSORTIUM

2023 TAC Areas of Focus

1. Project support, incl. cross-project coordination/communication
   a. Outcomes: adoption of common code, modules, patterns. Metrics needed. Dev velocity.
2. **Project Portfolio Growth**
   a. **Project Maturity and Adoption**
      i. **Maturity stage progression**
      ii. **Adoption: GH Stars; Contributor counts; Outreachy use; LF Sec tool; OSSF Scorecards**
         1. **Consider folding these into stage criteria and/or Growth Plan**
      iii. **Landscape**
   b. **Portfolio Growth (landscape)**
      i. **per qtr target TBD**
3. Cross-org coordination
   a. Outcomes
      i. NIST.. leading to recommendations to companies for adoption of CC technologies
      ii. Inclusion of CC in technologies considered by various organizations
   b. DARPA held a workshop on Dec 1-2 in San Francisco on “TEEs as SCIFs” to enable the government to share its vast troves of highly sensitive data with the broader community without exposing secrets. There will be follow-ups from that.
   c. Standards orgs: IETF, TCG, RISC-V, HomomorphicEncryption.org, …
   d. Open-source orgs: CNCF, TrustedFirmware.org, …
   e. Government agencies: NIST, BSI, …
   f. Academia: NSF Center for Distributed Confidential Computing, …

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing Summit

Raluca Ada Popa

CONFIDENTIAL COMPUTING CONSORTIUM

Conformance to terminology - Dave

Various examples across industry:

- IEC 62443
- Vendor self-assertion
- OCF: OCF-generated requirements and contracted certification
- IPv6Ready: IETF-generated requirements but external lab vendor certification
- DISA, NIST: Regulatory body requirements
- NISTIR 8259A: Regulatory body recommendations (not requirements)
- CCC Wikipedia article should follow TAC definitions
- …

Updates from Outreach Committee

- Landscape and solutions map - Ben Fischer
- 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
  - Alternate effort also do a confidential computing page
- https://en.wikipedia.org/wiki/Trusted_execution_environment
- New Website, status

CONFIDENTIAL COMPUTING CONSORTIUM

Formalization for GRC SIG?

- GRC SIG is not listed in the project matrix
  - project mentor
  - annual updates

- Any other formalization?

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
~~15 Dec 2022~~		
~~29 Dec 2022~~		~~Canceled~~
12 Jan 2023	Veracruz - Thomas?	EUAC FOSDEM Briefing
26 Jan 2023		
9 Feb 2023	Gramine - Michal, Mona, Don	
23 Feb 2023		

Next Agenda (2023-01-12)

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. Conformance to terminology - Dave Thaler
5. 2023 Goals
6. Community Architect Position
7. Annual Report from <?>
8. EUAC FOSDEM Briefing
9. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

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	Lily	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	15 SEP 2021	17 NOV 2022	Tate Tian	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	21 JUNE 2022
Veraison	Arm	4 FEB 2022	Yes	Yes	16 MAR 2022	18 May 2022	TBD	Howard Huang	NOV 2021

CONFIDENTIAL COMPUTING CONSORTIUM

Deferred topics / Backup

Tentative TAC Tech Talk topics

- Trust domains - Mike?
- Defined-Trust Transport (DeftT) Protocol for Limited Domains - Kathleen Nichols, Van Jacobson, Randy King
- CDCC research updates
- Relationship between eBPF and Confidential Computing - Dave Thaler

TAC Budget

Description	2022 Approved Budget	2022 September YTD	2023 Draft Budget	Notes	Area
License Scanning	$12,000	$0	$0		Project support
Test infrastructure (capital or non-capital)	$75,000	$9922	$60,000	$10k/project x 6 projects	Project support
IT Services and Collab Tools	$3,864	$6,507	$8,000	website, slack, groups,io	Project support Community development & DCI
Consortium IT Services and Collab Tools	$100,000	$0	$10,000	Misc. budget for use by projects	Project support
Travel expenses	$0	$0	$80,000	$10k/project x 8 projects	Project support Cross-org coordination
Software licenses	$10,000	$0	$0		Project support
Outreachy (internships/community support)	$52,000	$8,000	$32,000	Outreachy ($8k x 4 projects)	Community development & DCI Project support
Community management for projects			$100,000		Community development & DCI Project support
Subtotal	$257,781	$17,952	$290,000		

CONFIDENTIAL COMPUTING CONSORTIUM

Annual report

governance/project-progression-policy.md at main · confidential-computing/governance (github.com)

“The review includes the following:

1. Review whether any answers to the project's submission template or Technical Charter have changed, and if so, review the new answers. A representative from the project is responsible for presenting any deltas to the template answers since the last review, if any. If there are no changes, there is nothing to review here.
2. Review the project's progression status to determine whether the project is in the stage that accurately reflects its needs and goals. For example, is it already ready to move to another progression level? Is it on track at the current level? Is any action needed from the TAC (e.g., change in or addition to any project mentor(s))? If nothing has changed significantly, there may be nothing to review here.
3. Review any budget allocations relevant to the project, and whether any adjustments are needed.
4. Review license scans provided by the Linux Foundation. Provide feedback on any outstanding issues and evaluate the scanning service from the project's perspective.

Projects are encouraged to proactively inform the TAC when something changes that affects their submission template or Technical Charter (changing a License, security reporting process, CoC, etc.), rather than waiting for the next annual review.”

CONFIDENTIAL COMPUTING CONSORTIUM

Budget as of 9/30/2022

Description	2022 Approved Budget	YTD Actuals thru Sept 22	Sept 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	$6,507	$758	$3,790	
Non-Capital Equipment		$4,961	$0	-$4,961	Custom Exxact Workstation & Amazon order (Gramine)
Community Support	$0	$80	$0	$0	
Consortium IT Services and Collab Tools	$100,000	$0	$0	$100,000	
Hosting and other costs	$10,000	$0	$0	$10,000	
Internships	$52,000	$0	$8,000	$52,000	Outreachy
Subtotal	$257,781	$17,952	$8,758	$239,829	

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
- 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
-

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

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 $10K 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 Common Test Infrastructure

- **Summary:**
  - Projects preferred per project funding. No demand for common infrastructure. Approvals retained here for reference.
- **Needing**:
  - LF IT ready to meet for sizing and technical requirements
- Approved: 50K for infrastructure management and 15K for hardware
- Would any project use such infrastructure if it existed?
  - Projects: Enarx yes, OE no, Gramine no, **Occlum ?? (Annual Report)**

Reference Common Test Infrastructure

- **Summary:**
  - Projects preferred per project funding. No demand for common infrastructure. Approvals retained here for reference.
- **Needing**:
  - LF IT ready to meet for sizing and technical requirements
- Approved: 50K for infrastructure management and 15K for hardware
- Would any project use such infrastructure if it existed?
  - Projects: Enarx yes, OE no, Gramine no, **Occlum ?? (Annual Report)**