Technical Advisory Council (TAC) Meeting

January 25, 2024

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. Old Business
    a. Tech Talk: Kernel ABI & SIG (Dan Williams)
    b. Asia Friendlier Meeting Schedule (Mike Bursell)
    c. NIST RFI Responses (Mark N. & Sal)
    d. Scaling Project Mentors
3. New Business
    a. Announcements
    b. 2024 TAC Responsibilities
    c. NIST RFI Responses (Mark N. & Sal)
    d. New project onboarding
4. Future business
    a. Next meeting agenda
    b. Issues/Pull requests

Roll Call

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

* *TAC chair*

Member	**Representative / Alternate**	**Email**
Arm	Nathaniel McCallum	nathaniel.mccallum@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 Johnson	dan.middleton@intel.com
Microsoft	Alec Fernandez	alfernandez@microsoft.com
Red Hat	Lily Sturmann / Yash Mankad	lsturman@redhat.com

Welcome New Community Members

New to the community?

Haven’t introduced yourself at least twice?

Let us know

- your name, pronouns
- where you are joining from
- your main Confidential Computing interest

Old Business

Minutes for December 14, 2023

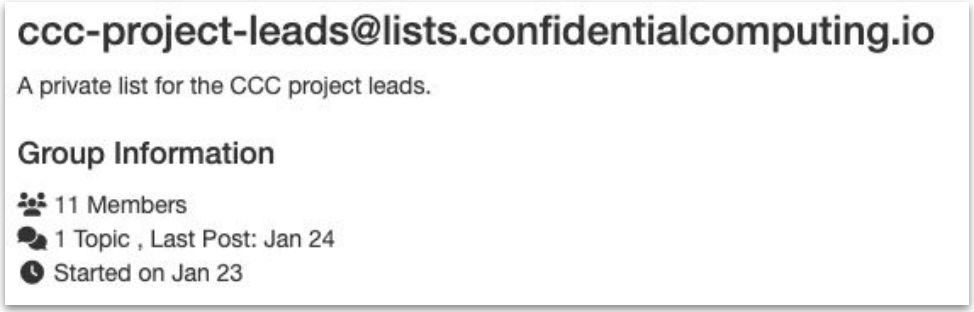
https://github.com/confidential-computing/governance/pull/209

- Coconut-svsm project proposal - APPROVED
- Kernel SIG proposal - APPROVED

How to scale Project Mentors as we add new projects:
https://github.com/confidential-computing/governance/issues/207

New Business

- Announcements:
  - Project Leads Mail List - Thanks, Lily!



- 2024 TAC Responsibilities
- RFI Responses (Mark N & Sal)

TAC Priorities

- Objectives and Key Results [doc]
  - Projects
  - Ecosystem
  - Community

By working together as a community we can make the world more secure with Confidential Computing than we could as individuals or individual companies.

A community focused on open source licensed projects securing DATA IN USE & accelerating the adoption of Confidential Computing through open collaboration

RFIs

https://lists.confidentialcomputing.io/g/tac/message/1254

Due January 15: NIST SP 1800-28 (Data Confidentiality: Identifying and Protecting Assets Against Data Breaches)
Due January 25: NIST SP 800-226 (Guidelines for Evaluating Differential Privacy Guarantees)
Due February 2: Safe, Secure, and Trustworthy Development and Use of AI

2024 TAC Objectives

Working document:

https://docs.google.com/document/d/1l5ekwOC0KhVwmBebaR9WHlFoCrM6mQEQolMo84-4kkk/edit

Food for thought (Thanks, Dave):

https://lists.confidentialcomputing.io/g/tac/topic/101726010#1137

https://wiki.lfnetworking.org/pages/viewpage.action?pageId=101352491

Next Agenda (2024-02-08)

1. Welcome, roll call, introduce any first-time attendees
2. Old Business
3. New Business
4. Project: Veracruz?
5. TAC Goals: Discuss Project and Community Goals
6. Tech Talk:
7. Any other business

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

Project	Last Annual Review	Next Annual Review	Mentor	Webinar
Enarx	2022-03-10		Nick Vidal	Jan 2021
OE SDK	2022-02-24		Dave Thaler	Mar 2021
Gramine	2023-02-09		Eric V	Feb 2022
Keystone	2023-02-23	2023-03-07	Lily	Jun 2021
Occlum	2022-11-17		Tate Tian	May 2021
Veracruz	2023-01-12		Thomas F	Apr 2021
Veraison	2023-06-15		Howard Huang	Nov 2021
VirTEE				
SPDM-RS				
Certifier Framework				
Coconut-SVSM			Alec Fernandez	

SIG / WG	Last Annual Review	Next Annual Review	Mentor	Webinar
CCC-Attestation SIG	2022-04-21		Dan	21 June 2022
GRC SIG	Quarterly 2023-10-08		Mark Novak	

Deferred topics / Backup

TAC Budget (Actuals through November)

Description	2023 Budget	Actuals through Nov	2023 Remaining	2024 Budget	Notes	Area
License Scanning	$0	$0	$0	$0	LF Security	Project support
Test infrastructure (capital or non-capital)	$60,000	$13,479	$46,521	$60,000	$10k/project x 6 projects	Project support
IT Services and Collab Tools	$15,000	$8,369	$6,631	$15,000	website, slack, groups,io	Project support Community development & DCI
Consortium IT Services and Collab Tools	$10,000	$0	$10,000	$10,000	Misc. budget for use by projects	Project support
Travel	$60,000	$17,678	$42,322	$60,000	$10k/project x 6 projects	Project support (combined with other travel)
Hosting and other costs	$306	$138	$168	$0	Software	Project support
Outreachy (internships/community support)	$32,000	$8,000	$24,000	$32,000	Outreachy ($8k x 4 projects)	Community development & DCI Project support
Community Support	$100,000	$0	$100,000	$100,000	Part-time Technical Architect	Community development & DCI Project support
Subtotal	$277,000	$47,664	$229,336	$277,000		

Any other business / Schedule

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk / Proposal / etc
23 Mar 2023	OE SDK - Radhika		SGX Assurance Tool - Alex Berenzon
6 April 2023	GRC - Mark Novak [3]	[2] Progression - Howard	CDCC - XiaoFeng Wang
20 April 2023		[1] Cross Project - Lily / EricV	
4 May 2023		[4] Education - Cfir et al	VirTEE - Sergio Lopez Pascual (@slp)
18 May 2023	Attestation SIG	[5] D&I - Dan & Nick	Keylime - Thore / Marcio
1 June 2023		[2] Progression pt.2 - Dave/Howard	Bao Project - Sandro / Howard
15 June 2023	Veraison - Thomas Fossati	[2] Progression pt.2 - Dave/Howard	
29 June 2023	CCS	CCS	CCS
13 July 2023		1, 3, or 4	~~Fan Zhang - CDCC second talk~~
27 July 2023	Canceled	n/a	~~SPDM - Jiewen Yao~~
10 Aug 2023	GRC Sig quarterly update	n/a	CHAOSS and D&I - Georg Link SPDM - Jiewen Yao
24 Aug 2023	Outreach update	All / Quarterly Checkup	CISA RFI

1. we increased Cross-project Integration [Lily, EricV]
2. the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]
3. other organizations reference Confidential Computing [MarkN, Howard, Thomas]
4. grew outbound education [Giuseppe, Cfir, EricN]
5. matured community D&I [Dan, Nick]

Any other business / Schedule (Continued)

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk
07 Sept 2023			MPC/FL + TEE and FHE - Kevin (Inpher)
21 Sept 2023			Oblivious RAM: from theory to large-scale real-world deployment - Elaine Shi (Carnegie Mellon University)
05 Oct 2023	Certifier Framework	2024 Planning	
19 Oct 2023	Certifier Framework	2024 Planning	
02 Nov 2023	Islet	2023 Grading	S/W Supply Chain - Marcela Melara
15 Nov 2023	FYI ONLY - LAST BOARD MEETING OF 2023 - QUEUE UP ANY VOTES WE NEED BEFORE THEN		
16 Nov 2023	Outreach/TAC goal sync	Cross-Project Survey (Lily)	Common API (Wenhui and Ken)
30 Nov 2023	COCONUT-SVSM	Islet	
14 Dec 2023	COCONUT-SVSM	Kernel SIG	Kernel ABI (Dan Williams)
28 Dec 2023	Canceled		

1. we increased Cross-project Integration [Lily, EricV]
2. the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]
3. other organizations reference Confidential Computing [MarkN, Howard, Thomas]
4. grew outbound education [Giuseppe, Cfir, EricN]
5. matured community D&I [Dan, Nick]

Attestation Wikipedia Article

Where do we want to do this?

- TAC
- AAA SIG ←
  - Work offline, mail list, updates in the SIG, etc.
- …

Are there other groups we should involve?

- TCG (Henk volunteered)
- …

Project Website Funding

Gramine and Veraison have both asked for website updates

- Rough estimate approximately $5K each ($16k for github page)
- Existing budget allocated $10K total for all projects for “Project IT Services and Collab Tools” which would cover website redesign
- Gramine also needing VPS Cloud services from the same budget item

1) Gramine VPS could be funded out of “Test Infrastructure/Hardware” budget ($10K) and that would allow all the 10K from Project IT Services to be used on websites
2) The TAC could get Governing Board approval for additional funding for Project IT Services
3) The TAC could also/instead get approval to allow funding to be shifted from Test to IT
4) Seek competitive bid from outside LF?
5) Associate this spend level with progression level

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
  - Slack
- Optional security scanning
- LFX tools (https://lfx.linuxfoundation.org)

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 LFX mentorship
- 2022-03-10: Overview of TCG confidential computing
- 2022-04-07: Governance
- 2022-04-21: Code Scanning via LFX Security
- 2022-05-05: IETF Trusted Execution Environment Provisioning (TEEP)
- 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
- 2022-09-22:
- 2022-10-06: HC / RISC-V Security
- 2022-12-01: Best Practices for Creating an Inclusive Community
- 2023-02-25: RISC-V AP-TEE
- 2023-03-09: eBPF
- 2023-03-23: SGX Assurance Tool

Annual reports

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.”

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