Technical Advisory Council (TAC) Meeting

March 07, 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
3. New Business
    a. Announcements
        - Second session of Kernel SIG this Friday.
        - OC3 is next week. Any last minute items?
        - Our 3/21 meeting is during Kubecon. Do we want to cancel?
    b. Keystone annual update
    c. Glossary
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
TikTok	Mingshen Sun / Yao Zhang	mingshen.sun@tiktok.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

- https://github.com/confidential-computing/governance/pull/222/files

New Business

- Projects
  - Keystone - Annual Review
- Ecosystem
  - Glossary
    - https://github.com/confidential-computing/glossary created
    - requested registration of glossary.confidentialcomputing.io
- Community
  - .
- TAC Schedule
  - Populate schedule for Goals and Tech Talks

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

Project	Last Annual Review	Next Annual Review	Mentor	Webinar
Enarx	2022-03-10	2024-04-04	Nick Vidal	Jan 2021
OE SDK	2023-03-23	2024-04-18	Alec Fernandez	Mar 2021
Gramine	2023-02-09		Eric V	Feb 2022
Keystone	2023-02-23	2024-03-07	Lily	Jun 2021
Occlum	2022-11-17	2024-3-21	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				
Islet				
Coconut-SVSM			Alec Fernandez	

SIG / WG	Last Annual Review	Next Annual Review	Mentor	Webinar
CCC-Attestation SIG	2022-04-21		Dan	21 June 2022

Topic Schedule

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2024-02-08		**Mentorship (Yash/Lily)**	
2024-02-22			
2024-03-07	**Keystone**	**Ecosystem/Terminology (MikeB)**	
2024-03-21	**Occlum**	**Ecosystem/Compliance (Mark N)**	
2024-04-04			**virTEE Demo**
2024-04-18	**OE SDK**		
2024-05-02			
2024-05-16			
2024-05-30			
2024-06-13			
2024-06-27			
2024-07-11			
2024-07-25			

Topic Schedule: Continued

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2024-08-08			
2024-08-22			
2024-09-05			
2024-09-16			
2024-10-03			
2024-10-17			
2024-10-31			
2024-11-14			
2024-11-28			
2024-12-12			

TAC February Discretionary Budget Update

Budget Category	Budget	Spent/Forecast	Remaining	Notes
Travel	$59,500	$0	$59,500	~8.5k per project
Test Infrastructure	$59,500	$2,250	$57,250	~8.5k per project
Consortium IT Services and Collab Tools	$9,996	$0	$9,996	~1.4k per project
Internships	$32,000	$1,500	$30,500	

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

Thank You.