Technical Advisory Council (TAC) Meeting

May 30, 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. Announcements: None
3. Old Business - Recap May 16 meeting
4. New Business
   a. ~~TAC Goal: Roots of Trust, Nathaniel~~
   b. CC Summit items
   c. Tech Talk: “TPMs, Merkles.., TEEs…”, Marcela & Chad
5. Future business
   a. Next meeting agenda 6-13
      - TBA, John or Nathaniel
      - Post Quantum, Hart Montgomery
   b. Backlog
      - Barriers to Adoption; Glossary (tbd)
      - Budget (tbd); Issues/Pull requests

Roll Call

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

* *TAC chair*

Member	**Representative / Alternate**	**Email**
AMD	David Kaplan / Harold Gilkey	david.kaplan@amd.com
Arm	Nathaniel McCallum	nathaniel.mccallum@arm.com
Google	Catherine Zhang	cxzhang@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton * / Simon Johnson	dan.middleton@intel.com
Meta Platforms	Henry Wang / Kevin Hui	kevinhui@meta.com
Microsoft	Alec Fernandez	alfernandez@microsoft.com
Nvidia	Fritz Alder	falder@nvidia.com
Red Hat	Yash Mankad / Ram Pai	ymankad@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

1. Tech Talk: PDaP: Privacy-preserving Data Sharing in Practice (NSF/OSTP)
2. Announcements
    a. Mentorship PR merged
    b. CCC Brand repositioning Working group
    c. CC Conformance / Certification
3. TAC Goals:
    a. TAC Goals (Dan)

TAC Goal Topic: Roots of Trust, Nathaniel

TAC Tech Talk

TPMs, Merkle Trees and TEEs: Enhancing SLSA with Hardware Assisted Build Environment Verification,

Marcela Melara & Chad Kimes

Announcements

- Mentorship PR Merged
- Repositioning WG
  - Discussed the Brand repositioning of the Confidential Computing Consortium
  - Ab Nacef from AMD offered to lead the initiative
  - The Kick off meeting following today's TAC meeting
  - Please sign up to participate in the working group
- Conformance WG
  - Please review the initial proposal for a working and signup to participate in the discussion
  - Confidential Computation Conformance Working Group

CC Summit Preview

CCC Booth

- **Projects/SIG demo + Member participation + Digital slideshow**

On stage

- **Keynote** “**Advancing Confidential Computing And Its Ecosystem**” - Mike Bursell, CCC
- **Regulations panel: “Regulations And Confidential Computing In AI Use Cases Panel** - moderated by Sal Kimmich, CCC
- **Breakout 1: “Auditable and Verifiable Transparency with Trusted Execution Environment”** - Mingshen Sun (TikTok)
- **Breakout 2: “Enhancing End-User Devices with Confidential Computing: Protecting AI Applications & Improving Gaming Experiences”** - Heeill Wang, Mete Ozay (Samsung)
- **Poster Panel In-person + recording** (moderated by Mike Bursell + CCC members)

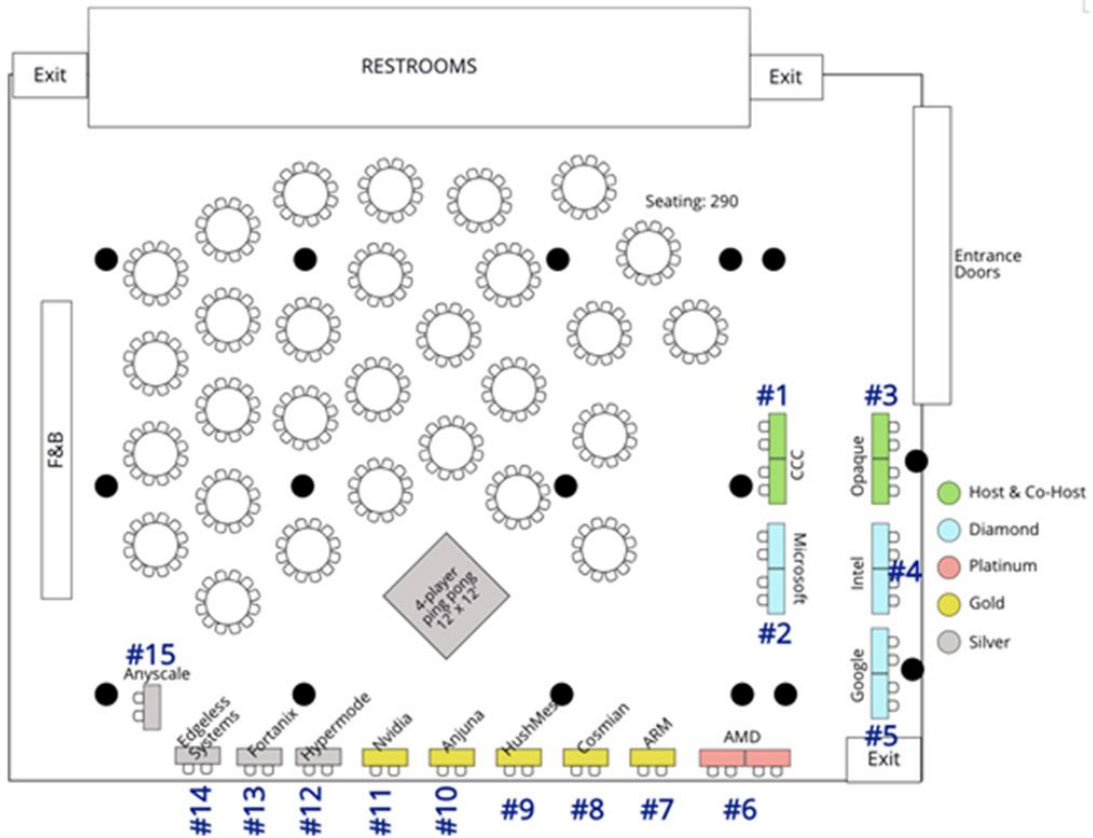
Session chairs: Mike, Sal, Kate, Leo are chairing keynote and breakout sessions

CCC Member Happy Hour 🍸

Bourbon & Branch - June 4 | 6pm RSVP link

CC Summit Onsite Layout

Exhibits Floor Plan:



CONFIDENTIAL COMPUTING CONSORTIUM

Invite your network to CC Summit

CCC 50% Discount Promo Code: CCC50

Registration Link

Meet us at CCC Member Happy Hour

Speakeasy place.
Free, but must RSVP.

RSVP Link

CONFIDENTIAL COMPUTING CONSORTIUM

Events Speakership Call For Proposal

Submit Your Content & Speaker Interest

PET Summit APAC: **(deadline 6/13)** Pre-set topics, members in APAC. July 16, 2024 | Singapore **deadline moved-up

OSS EU CC Mini Summit: **(deadline: 8/8)** September 19, 2024 at 13:30 - 17:00 CEST | Vienna, Austria

TAC Goals

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

Projects

Project	Last Annual Review	Next Annual Review	Mentor	Webinar	
Enarx	2024-04-04		Nick Vidal	Jan 2021	added to invite
OE SDK	2024-04-18		Alec Fernandez	Mar 2021	added to invite
Gramine	2023-02-09		Eric V	Feb 2022	
Keystone	2024-03-07		Lily	Jun 2021	added to invite
Occlum	2024-03-21		Tate Tian	May 2021	requested
Veracruz	2023-01-12		Thomas F	Apr 2021	
Veraison	2023-06-13		Howard Huang	Nov 2021	
VirTEE			Yash Mankad		
SPDM-RS			Fritz Alder		
Certifier Framework					
Islet					
Coconut-SVSM			Alec Fernandez		

SIGs

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	
Kernel SIG	Launched Q1'24		TBD	

Project Pipeline

Onboarded \o/

- VirTee Proposal, Charter, Contribution Agreement
- spdm-rs Proposal, Charter, Contribution Agreement Not Required
- Certifier Framework Proposal, Charter, Contribution Agreement Not Required
- Islet Proposal, Charter, Contribution Agreement
- Coconut-SVSM Proposal, Charter, Contribution Agreement

In Progress

-

Ready For Vote

-

* Project Status Board https://github.com/orgs/confidential-computing/projects/2

SIG Events Call For Proposal

Submit Your Content & Speaker Interest

PET Summit APAC: **(deadline 6/18)** Pre-set topics, members in APAC. July 16, 2024 | Singapore

OSS EU CC Mini Summit: (deadline: 8/8) September 19, 2024 at 13:30 - 17:00 CEST | Vienna, Austria

TAC March Discretionary Budget Update

Budget Category	Budget	Spent/Forecast	Remaining	Notes
Technical Community Architect Travel	$45,500	$2,172	$43,328	
Travel	$14,000	$6,402	$7,598	~2k per project
Test Infrastructure	$59,500	$5,712	$53,788	~8.5k per project
Consortium IT Services and Collab Tools	$9,996	$0	$9,996	~1.4k per project

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	2024 TAC Objectives	
2024-03-21	Occlum		Payload Governance Patterns
2024-04-04	Enarx		virTEE Demo
2024-04-18	OE SDK		
2024-05-02		Yash - Internship/mentoring	UEFI, Dionna Glaze
2024-05-16		Revisit OKRs (Dan)	PDaP: Privacy-preserving Data Sharing in Practice James Joshi
2024-05-30		Nathaniel McCallum - Roots of Trust?	TPMs, Merkle Trees & TEEs, Marcela & Chad
2024-06-13		Alec Fernandez	Post Quantum - Hart Montgomery
2024-06-27		Zhipeng (Howard) Huang	
2024-07-11		Henry Wang / Kevin Hui	
2024-07-25		Catherine Zhang	

Topic Schedule: Continued

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2024-08-08		**Henry Wang / Kevin Hui**	
2024-08-22		**Catherine Zhang**	
2024-09-05		**Yash Mankad /Ram Pai**	
2024-09-19		**Fritz Alder**	**Collaborative and Private Data Processing with TEE-enforced Sticky Policy (LIN, Zhiqiang)**
2024-10-03		**Mingshen Sun / Yao Zhang**	
2024-10-17			
2024-10-31			
2024-11-14			
2024-11-28			
2024-12-12			

Internship / Mentoring

Program

- Similar to CNCF's lfx-mentorship
- We need project ideas that could be roughly completed in a 12-week work block, a willing mentor able to devote sufficient time to assisting a mentee complete the idea implementation, and set of required mentee skills.
- Project idea template will be similar to CNCF. (Some examples from their 2024 Summer Term: Thanos, Kubescape, Cilium)
- Projects should submit their project ideas as a Pull Request on CCC's mentorship repo (WiP - Sal's PR#223)

Internship / Mentoring

Est. Schedule

- **Proposed Term: July 15th - October 15th**
- CCC Projects idea submission deadline: **June 1st**
- Mentorships available on LFX Mentorship: **by June first week**
- Mentee applications open on LFX: **approximately 4 weeks (by July first week)**
- Mentee application review and acceptance: approximately during the **2 weeks before the term** begins. (**July 1 - July 15**)

Plan / Action(s)

- Projects / willing mentors to submit ideas to project lead mailing list for now, and as a PR once GH Mentoring repo is ready
- Yash and Riaan to meet with Ali Ok (who runs the CNCF Mentoring Program with Nate W) to finalize the schedule for CCC's Mentoring term.
- TAC members are requested to review Sal's PR#223 to complete the CCC Mentoring Github pages.
- Yash to work with Kate and Outreach team to advertise Mentoring Program to the right audience via appropriate channels and invite Mentees to apply once submissions are on the LFX Portal.

Thank You

CONFIDENTIAL COMPUTING
CONSORTIUM