Technical Advisory Council (TAC) Meeting

October 31, 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 - Recap last meeting
3. Announcements
    a. Elections
    b. Kubecon activities
    c. Project Mentorship Opportunities
    d. TAC Chair Election
    e. Face to face at FOSDEM
4. New Business
    a. OKR updates - Each TAC Member
    b. 2025 Planning - Each TAC Member
    c. Tech Talk Recap - Open HCL - Caroline
    d. Budget - Last call for changes
5. Future Business
    a. Next meeting agenda
        - 2025 Planning - Finalize
    b. Backlog

Roll Call

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

* *TAC chair*

Member	**Representative / Alternate**	**Email**
AMD	Nathaniel McCallum / David Kaplan	Nathaniel.McCallum@amd.com
Arm	Paul Howard	Paul.Howard@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

Last meeting:

1. CC Brand Repositioning WG Update
2. Budget Update and 2025 Budget

Announcements

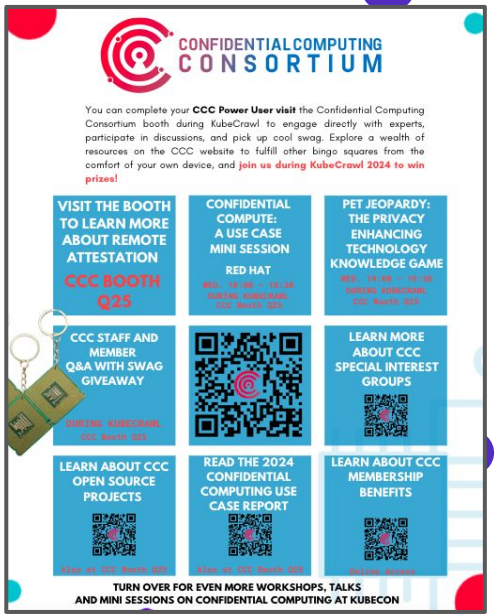
- The **Technical Advisory Committee elections** will take place in November
- Nominations for Chair and Co-Chair by 1 November
- PLEASE NOTE:
  - Nominations for General Member rep on the GB is also still open

Announcements

KubeCon Salt Lake City

CCC have a booth at Kubecon and a lot of incredible CC coverage this year. (tentative full schedule available here).

Booth Coverage is complete! Final schedule, talks and mini sessions will be sent to the mailing list today, and are represented on our "Confidential Computing Power User Bingo" style and complete schedule available now. Direct link to view and edit available here.



Announcements

KubeCon Asset Side 1: KubeCon Talks and Workshops on Confidential Computing

1. **From Silicon to Service: Ensuring Confidentiality in Serverless GPU Cloud Functions (NVIDIA)**
   - **Time:** Thu. 11:00 AM - 11:35 AM, **Location:** Salt Palace | Level 1 | 151 G
2. **Privacy in the Age of Big Compute (Confidential Computing Consortium)**
   - **Time:** Fri. 4:00 PM - 4:35 PM, **Location:** Salt Palace | Level 1 | Grand Ballroom A
3. **Confidential Containers 101: A Hands-on Workshop (Microsoft)**
   - **Time:** Wed. 2:30 PM - 4:00 PM, **Location:** Salt Palace | Level 1 | Grand Ballroom G
4. **Remote Attestation Using Veraison: Live 10 Minute Open Source Project Demo (Linaro)**
   - **Time:** Wed. 10:45 AM - 12:45 PM, Thu. 10:45 AM - 12:45 PM, **Location:** CCC Booth Q25
5. **Confidential Compute: A Use Case Mini Session (Red Hat)**
   - **Time:** Wed. 6:00 PM - 6:30 PM, Thu. 2:30 PM - 4:30 PM, **Location:** CCC Booth Q25
6. **Confidential Collaborative AI (Ultraviolet), Time:** Wed. 4:00 PM - 4:30 PM, **Location:** CCC Booth Q25
7. **Protecting LLMs with Confidential Computing (Ultraviolet)**
   - **Time:** Thu. 4:30 PM - 5:00 PM, **Location:** CCC Booth Q25
8. **Security Mini-Talk on Remote Attestation** (Anjuna)
   - **Time:** Wednesday, 2:45 PM – 3:15 PM, **Location:** CCC Booth Q25

Islet: LF Mentorship Opportunity!

Islet Mentorship: Strengthening Security through Fuzz Testing
Enhance **Islet's security** by identifying vulnerabilities early using **fuzz testing**. This project will integrate **Cargo Fuzz** tools with Islet's **CI pipeline**, focusing on testing **RMM interfaces** (RMI and RSI) based on ARM's RMM specification.

Scope of Work:

- **Phase I**: Develop 12 fuzz test harnesses using **Miri-based tests** (2 weeks), followed by a **1-week testing campaign**.
  - Miri Test Reference
- **Phase II**: Build advanced tests using **ACS-Test suite** (4 weeks), with 2 additional weeks for testing.

Outcome:
Deliver a set of **robust fuzz tests** integrated into Islet's CI, improving security and compliance with ARM standards.

Skills Needed: **Rust programming**, fuzz testing, and familiarity with **confidential computing, virtualization, and ARM architecture** is *extremely helpful* but not required.

Veraison: LF Mentorship Opportunities!

Veraison Mentorship #1: Enhancing CoRIM Support
This project will strengthen Veraison **CoRIM (Concise Reference Integrity Manifest) support** by integrating built-in object security and expanding signing capabilities. Participants will learn to generate and manage CoRIMs while building enhanced security into Veraison's services.

Scope of Work:

- **Familiarize** with the RATS architecture and CoRIM specifications.
- **Setup Veraison services**, deploy, and explore the REST API.
- Use the **cocli tool** to generate and manage CoRIMs.
- **Add signed CoRIM support** to Veraison services, enhancing security.

Stretch Goals: Enable **multi-signer support** for CoRIMs, Update the **CCA scheme** to incorporate multi-signatures.

Outcome: Deliver **robust CoRIM security features**, integrated into Veraison's services, improving integrity verification through enhanced signing and object security.

Skills Needed: Knowledge of **RATS architecture**, CoRIM, and API interaction, Experience with **Go** or relevant languages will be helpful.

Veraison: LF Mentorship Opportunities!

Veraison Mentorship #2: Harmonizing Open-Source Verifiers with RATS Standards

This mentorship focuses on **harmonizing Verifiers** with the RATS model, proposing standards for media types, evidence, and attestation results. Participants will align open-source Verifiers and propose ways to integrate **Keylime** for seamless interoperability.

Scope of Work:

- Define **media types for evidence** (e.g., TPM logs, incremental evidence).
- Standardize **attestation results** with EAT (Entity Attestation Token).
- Develop a **proposed adoption path** for integrating Keylime.

Stretch Goals: Create **CoRIM and policy formats** for runtime and UEFI boot attestation, Propose **policy primitives** for secure UEFI policies.

Outcome: Deliver **standardized evidence formats and adoption paths**, ensuring Verifiers across different open-source projects work seamlessly within the RATS model.

Skills Needed: Familiarity with **RATS architecture** and attestation workflows, Knowledge of **policy management** and TPM evidence formats.

Announcements

FOSDEM February 1-2 @ Brussels

- Interest in face to face at FOSDEM from Attestation SIG.
- What about TAC?

TAC September Discretionary Budget Update

Budget Category	2024 Budget	Actuals	Forecast	Remaining
TCA Travel	$45,500	$7,950	$0	$37,550
Travel	$14,000	$6,584	$0	$7,416
Test Infrastructure	$59,500	$1,212	$4,500	$53,788
Consortium IT Services and Tools	$9,996	$0	$0	$9,996

TAC Budget Proposal 2025 - Under GB Consideration

Budget Category	2024 Budget	Actuals	Forecast	Remaining	2025 Budget
TCA Travel	$45,500	$7,950	$0	$37,550	$20,000
Travel	$14,000	$6,584	$0	$7,416	$14,000
Test Infrastructure	$59,500	$1,212	$4,500	$53,788	$45,000
Consortium IT Services and Tools	$9,996	$0	$0	$9,996	$0
Mentorship	$32,000	$0	$1,500	$30,500	$18,000
	$160,996	**$15,746**	**$6,000**	**$139,250**	**$97,000**

Open Items: Lab .. Virtual or Physical providing bare metal access to Projects, Universities, member companies?

Consider project portfolio growth

Projects

Project	Last Annual Review	Next Annual Review	Project Liason	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 Stuurman	Jun 2021	added to invite
ManaTEE	2024-07-25		Dayeol Lee		
Occlum	2024-03-21		Tate Tian	May 2021	requested
Veracruz	2023-01-12		Thomas Fossati	Apr 2021	
Veraison	2024-08-08		Howard Huang	Nov 2021	Invitation accepted
VirTEE	2024-01-17		Yash Mankad		
SPDM-RS	2024-01-17		Fritz Alder		
Certifier Framework	2024-01-17				
Islet	2024-03-01		Bokdeuk Jeong		

SIGs

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

Topic Schedule

2024-09-05		**Yash Mankad / Ram Pai (Mentorship)**	**Super Tech Talk - Andrey Pogoreltsev - CTO of Super Protocol**
2024-09-19	**Linux Plumbers conflicts?**	?	**- Collaborative and Private Data Processing with TEE-enforced Sticky Policy (Zhiqiang Lin)** **- Research topic: Formal programming techniques for secure data processing) by Patrick Eugster**
2024-10-03	**Rosh Hashanah conflicts?**	?	**- Chandra Nelogal: Extending Confidentiality to Data Storage** **- Caroline Perez-Vargas: Project presentation**
2024-10-17		~~David Kaplan (Plumbers recap)~~	
2024-10-31		OKR Updates - ALL TAC MEMBERS	2025 Planning
2024-11-14		**2025 Planning**	Islet Tech Talk - Bokdeuk Jeong
2024-11-28	**US Thanksgiving Conflicts**	**Cancel**	**Cancel**
2024-12-12			Tech Talk: UCLA Trustworthy AI Lab: guangcheng@g.ucla.edu - Guang Cheng

Thank You

CONFIDENTIAL COMPUTING
CONSORTIUM