Technical Advisory Council (TAC) Meeting

October 03, 2024

CONFIDENTIAL COMPUTING CONSORTIUM

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. TAC Chair Election
4. New Business
    a. Tech Talk - Chandra Nelogal
        - Extending Confidentiality to Data Storage

    b. Attestation Terminology - Who or what is in my TCB?

    c. Tech Talk - Caroline Perez-Vargas
        - Open HCL

5. Future Business
    a. Next meeting agenda
        - Budget
        - Linux Plumbers Conf. recap - David Kaplan
    b. Backlog
        - 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

Last meeting:

1. Tech Talk - Zhiqiang Lin
   a. Collaborative and Private Data Processing with TEE-enforced Sticky Policy
2. Tech Talk - Patrick Eugster
   a. Formal programming techniques for secure data processing
3. Repositioning WG - Ab Nacef
4. Attestation Terminology

Announcements

KubeCon Salt Lake City

CCC have a booth at Kubecon and would like to invite members an projects to staff the booth, giving them the opportunity to talk about their work as well as their involvement in CCC.

Please reach out to Riaan to get on to the schedule (tentative full schedule available here).

Booth Coverage Times Still Needed:

- **Wednesday, Nov 13**
  - **6:30 PM – 8:00 PM**: Booth Coverage Needed during KubeCrawl, great time to a bigger new audience
- **Thursday, Nov 14**
  - **2:30 PM – 4:30 PM**: Booth Coverage Needed
- **Friday, Nov 15**
  - **10:30 AM – 12:30 PM**: Booth Coverage Needed
  - **12:30 PM – 2:30 PM**: Final Booth Coverage and Passport Redemption (B

Announcements

KubeCon is a great opportunity for 15 minute demos or use cases (open to remote/recorded sessions from members)

Demos and Mini-Sessions:

- **Demos:**
  - **Arm/Intel Demo**: Thursday, 12:00 PM – 12:30 PM (Need to confirm speakers and details)
  - **Anjuna Security Mini-Talk on Remote Attestation**: Wednesday, 2:45 PM – 3:15 PM
- **Mini-Sessions:**
  - **Attestation and Trust**: Intel session, Thursday 3:00 PM – 3:30 PM (Need additional speakers and participation)
  - **Confidential AI Discussion**: Wednesday, 4:00 PM – 4:30 PM (Still looking for participants)

KubeCon Talk and Engagement Ideas:

- **Daily Secret Code Giveaway**: Each talk reveals a cryptographic phrase that attendees bring to the booth to unlock swag or enter raffles. These should all combine to a

-
-

Announcements

- The **Technical Advisory Committee elections** will take place in November
- We need nominees for the Committee Chair for 2025
- All premier members reps are eligible vote for candidates
- More information to follow in on the TAC mailing list

Thank you to Dan for your service in 2024 - Not done yet!

Announcements

The Brand Repositioning WG have created a document to solicit feedback for potential CC supply chain use cases.
This is a reminder to the members to share their input.

https://docs.google.com/document/d/1yYwIB07OgFfpbxk2KvmI3goKBdqxZTc0MkpmGzCkuvM/edit#heading=h.1cwejrcpvn82

Tech Talk

Extending Confidentiality to Data Storage

Chandra Nelogal

Attestation & AVS questions

Business models doc encouraged lots of discussion. Key technical questions:

- Do we need to add “remote” to the CCC definition of CC? *(Consensus: yes, but…)*
  - …do we need to work with IETF to define remote attestation better?
- Define:
  - Attestation Verification Service (AVS)
  - Workload ← **Re-opened at Attestation SIG**
  - Endorsement, endorser
  - TEE
  - …
- AVS-specific
  - What service characteristics are MUST/SHOULD/MAY for an AVS to provide
  - Are there use cases to run an AVS which is not workload-aware?
  - Describe different policies that might be relevant to an AVS
  - AVS trust relationships:
    - How can an AVS prove that it should be trusted?
    - OR What evidence should a relying party accept to establish a trust relationship to an AVS?
- What entities may a relying party wish to remove from their trust chain? ← **Mail List discussion**
- **BONUS**: Clear need to describe and classify different models for CC with Linux Containers

CONFIDENTIAL COMPUTING CONSORTIUM

Attestation & AVS questions

What entities may a relying party wish to remove from their trust chain? ← **Mail List discussion**

Subtext?: What if the CSP operates the AVS?

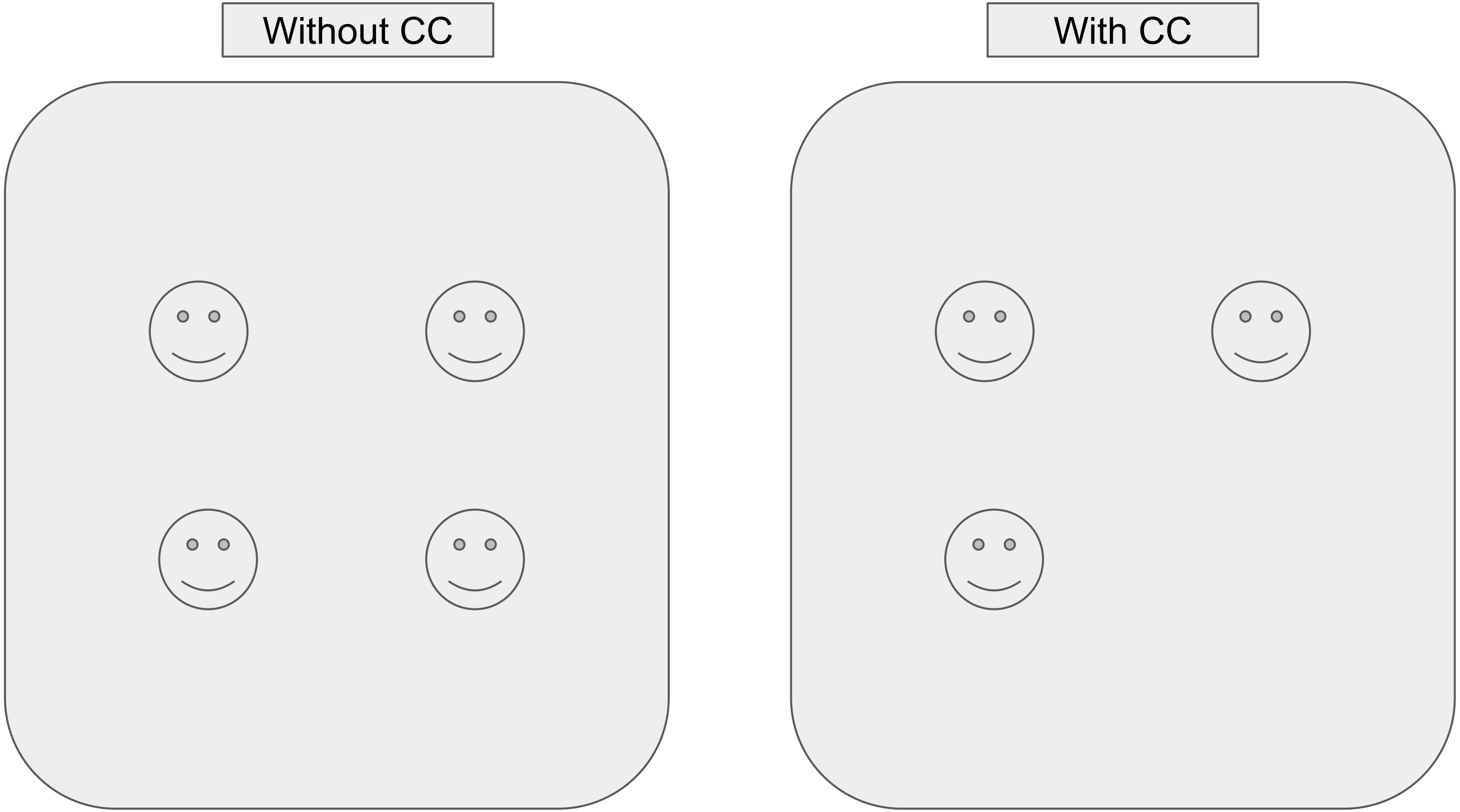
Variants: Is the CSP in ~~the TCB~~ your trust boundary? How much of the CSP? Can I have my Managed Services and eat them too?

Mail list: Turtles / CSP->Auditor; Separation of Duties;

Approaches to Enumerating the Entities:

Enumerate Software; Attestation Values; Services/Operational Roles;

IAAS	PAAS	SAAS	FAAS



Without CC

With CC

Can we get to a description like this?

Tech Talk

OpenHCL

Caroline Perez-Vargas

CONFIDENTIAL COMPUTING CONSORTIUM

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
Occlum	2024-03-21		Tate Tian	May 2021	requested
Veracruz	2023-01-12		Thomas Fossati	Apr 2021	
Veraison	2023-06-13	2024-08-08	Howard Huang	Nov 2021	Invitation accepted
VirTEE			Yash Mankad		
SPDM-RS			Fritz Alder		
Certifier Framework					
Islet			Bokdeuk Jeong		
Coconut-SVSM			Alec Fernandez		

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	
Kernel SIG	Launched Q1'24		Catherine Zhang - tentative	

TAC September Discretionary Budget Update

Budget Category	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

Topic Schedule

Date	CCC Project Topic	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2024-07-25	**Data Clean room cont.**	**Catherine Zhang (Kernel SIG - Rebranding? Conformance?)**	**Post Quantum - Hart Montgomery; AI / OPEA Zhiwei Zhang**
2024-08-08		**Fritz Alder (Academia & Tech Talks)**	**Runtime Attestations - Jason Rogers - Invary**
2024-08-22	**Tech Talk: OPEA project**	**Mingshen Sun / Yao Zhang (TBD)**	**Pandora: Principled Symbolic Validation of Intel SGX Enclave Runtimes (Jo Van Bulck)**
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		**Zhipeng (Howard) Huang (TBD)**	
2024-11-14		**Nathaniel (Roots Of Trust?)**	
2024-11-28	**US Thanksgiving Conflicts**	**?**	**?**

CONFIDENTIAL COMPUTING CONSORTIUM

Thank You

CONFIDENTIAL COMPUTING CONSORTIUM