Technical Advisory Council (TAC) Meeting

July 11, 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 last meeting
4. New Business
    a. Project proposal
    b. TAC Goals - Henry & Kevin
5. Future business
    a. Next meeting agenda
    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

Last meeting:

1. GRC: Mark Novak / Alec Fernandez
2. Data Cleanroom Project proposal

TAC Project Proposal

Data Clean Room Proposal

Vini Jaiswal, Dayeol Lee, Mingshen Sun

TAC Goals: Henry & Kevin

Draft Ideas For Feedback

- Open Sourcing Attestation Library
- Providing code transparency for our TEEs that we host on our datacenters,

Announcements

Update

NIST that may be of interest to us for review/responses/etc.

- Internal Report 8505 (Initial Public Draft)
- “A Data Protection Approach for Cloud-Native Applications”
  - From the abstract: “This document … provides a framework for aligning data protection approaches with the unknowns of data in transit. Specifically, it explores service mesh architecture, leveraging and emphasizing the capabilities of WebAssembly (WASM) in ensuring robust data protection as sensitive data is transmitted through east-west and north-south communication paths.”
  - Despite its encompassing title, the report is rather narrowly scoped to use of WASM to “address the need for data categorization during travel across services” and then using WASM to perform tasks around dynamic data masking, behavior analytics and DLP.
  - So while this particular report is of little interest to CC, there is definitely scope for NIST to publish a separate report with a similar title, but focused on use of Confidential Computing in cloud-native applications.

Announcements

Update

NIST that may be of interest to us for review/responses/etc.

- Internal Report 8517 (Initial Public Draft)
- “Hardware Security Failure Scenarios: Potential Weaknesses in Hardware Design”
    - This document is quite generic in nature but may have areas that could be updated specifically for Confidential Computing – e.g. section 5.11 on “Privilege Separation and Access Control Issues” which mentions two classes of vulnerabilities: “Confused Deputy” and “”Insecure Security Identifier Mechanism”. A separate analysis could be done about vulnerabilities specific to Confidential Computing and results shared with NIST.

Announcements

Update

NIST that may be of interest to us for review/responses/etc.

- Special Publication 1800-36 (Initial Public Draft)
- “Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Manag[illegible]nt: Enhancing Internet Protocol-Based IoT Device and Network Security”
  - The SP talks about two classes of issues: network-layer onboarding of devices (done through “attesting and verifying the identity and posture of the device and the network before providing the device with its network credentials”) and “scalable, automated mechanisms” for managing “IoT devices throughout their lifecycles”. Both of these operations are significantly aided by Confidential Computing, which may effectively remove the need to worry about a device and only worry about the code executing on that device, perhaps augmented with some device metadata such as its location and unique identifier.
  - There is only one mention of Trusted Execution Environment in the entire 5 parts of this sprawling SP, in part B, section H.1.1, bullet 5 of the document, focusing specifically on unique device credentials and nothing else. There are however mentions of Attestation (in Sections 7.7 and 7.8, also in Part B, and in Sections 2.1.4 and 2.4 in Part E), but nothing specifically tied to attesting code running in TEEs, which I think is an oversight.
  - Perhaps the response to this SP might include discussions specific to Confidential Computing and its unique properties, which, thanks to innovations such as ARM CCA, Keystone and others, are now available to IoT designers worldwide.

Events Speakership Call For Proposal

Submit Your Content & Speaker Interest

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

- Call for a Panel on the Technical Landscape of Open Source Confidential Computing

4 upcoming CFPs

- Cyber Security World: Oct 9-10, Singapore
- SOSS FUSION: Oct 22 - 23, Atlanta, GA
- OSS Japan October 28-29 | Tokyo, Japan - closes 2024-07-07
- Kubecon NA - Closed

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	2023-08-08	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	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		Catherine Zhang - tentative	

TAC March Discretionary Budget Update

Budget Category	Budget	Actuals	Forecast	Remaining
TCA Travel	$45,500	$2,172	$0	$43,328
Travel	$14,000	$3,363	$3,065	$7,572
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 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			TPMs, Merkle Trees & TEEs, Marcela & Chad
2024-06-13		Roots of Trust, Nathaniel McCallum (resched from 5/30)	Post Quantum Cryptography - John Manferdelli Post Quantum - Hart Montgomery - Moved out to 25 July
2024-06-27		Mark Novak / Alec Fernandez (GRC)	Data Clean Room Proposal - Vini Jaiswal
2024-07-11		Henry Wang / Kevin Hui (TBD)	Review: Data Clean Room Proposal - Vini Jaiswal
2024-07-25		Catherine Zhang (Kernel SIG - Rebranding? Conformance?)	Post Quantum - Hart Montgomery; (TBD OPEA Project)

Topic Schedule: Continued

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk / Proposal / etc
2024-08-08		**Fritz Alder (Academia & Tech Talks)**	**Runtime Attestations - Jason Rogers - Invary**
2024-08-22		**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)**	
2024-09-19	**Linux Plumbers conflicts?**	?	**Collaborative and Private Data Processing with TEE-enforced Sticky Policy (LIN, Zhiqiang)**
2024-10-03	**Rosh Hashanah conflicts?**	?	**?**
2024-10-17		**David Kaplan (On Leave, Kernel SIG?)**	
2024-10-31		**Zhipeng (Howard) Huang (TBD)**	
2024-11-14		**Nathaniel (Roots Of Trust?)**	
2024-11-28	**US Thanksgiving Conflicts**	**?**	**?**
2024-12-12			

Thank You

CONFIDENTIAL COMPUTING
CONSORTIUM