Technical Advisory Council (TAC) Meeting

September 9, 2021

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.

CONFIDENTIAL COMPUTING CONSORTIUM

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.

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

1. Welcome, Roll call
2. Action item review
3. Upcoming events (LPC, OSSNA) and TAC meetings
4. Updates from Outreach committee
5. VOTEs:
    1. July 1 minutes
    2. July 15 minutes
    3. August 26 minutes
    4. Attestation SIG Chair (Aeva -> Larry)
    5. Diversity, Civility, & Inclusion policies (PR #83)
    6. Outreachy support
6. Confidential Computing definition perspective from AWS - Mike
7. Time permitting: Establishing common terminology (issue #79)
8. Any other business

Roll Call of TAC Voting Representatives

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

Member	**Representative**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Ant Group	Zongmin Gu	zongmin.gzm@antgroup.com
ARM	Thomas Fossati / Michael	thomas.fossati@arm.com
Facebook	Eric Northup / Shankaran	digitaleric@fb.com
Google	Iulia Ion	iuliaion@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton / Simon	dan.middleton@intel.com
Microsoft	Dave Thaler(*)	dthaler@microsoft.com
Red Hat/IBM	Lily Sturmann / Dimitrios	lsturman@redhat.com

**TAC chair*

CONFIDENTIAL COMPUTING CONSORTIUM

2. Action Item Review (1/2)

1. [Stephano] Process for doi assignment for whitepapers and CCC projects if they want one for a doc
2. [~~Mike~~, Simon, Stephen, ~~Zongmin~~, Grant] Please take either the inclusive open source community or inclusive speaker training with a view towards value for our projects
3. [Stephano] Look into any LF generated documentation around diversity and inclusion in general “style / inclusive writing guides”
    - https://developers.google.com/style/inclusive-documentation
    - https://docs.microsoft.com/en-us/style-guide/bias-free-communication
4. [Stephen] Chat with LF legal counsel to inform the process in place to establish a Vulnerability Management Team
5. [Ashley] Reach out to project mentors to confirm potential security contacts for each current and upcoming project
6. [Ben] Identify the TAM study discussed in the meeting in reference to maybe market metrics - DONE

CONFIDENTIAL COMPUTING CONSORTIUM

2. Action Item Review (2/2)

7. [Project Mentors] Recommend diversity and inclusion trainings to their projects and report back to the TAC on whether the maintainers or the contributors will be taking it and when the expected completion date is
8. [Ashley] Add to the outreach agenda discussion topic on inclusive orientation for webinar speakers- DONE
9. [Ashley] Identify link for the White Paper Google doc for updates and share with Thomas F. to provide suggested change - DONE
10. [Thomas F.] Suggest changes on the White Paper once Ashley has shared Google doc
11. [Ashley] Update Graphene to Gramine on the CCC website- DONE
12. [Ashley] Run vote for Occlum and Gramine to join the CCC during the first week of September (after Labor Day) – IN PROGRESS
13. [Ashley] Invite Gramine for a board presentation after OSS (next virtual board meeting) – IN PROG
14. [Thomas H] Support text creation for VM terminology (help Eric)

CONFIDENTIAL COMPUTING CONSORTIUM

Project	Proposed by	TAC Approved	Tech. Charter	IP Assigned	Board Presentation	Board Approved	Annual Review	Mentor	Webinar
Enarx	Red Hat	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	14 JAN 2021	Mike Bursell	JAN 2021
OE SDK	Microsoft	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	12 NOV 2020	Dave Thaler	MAR 2021
SGX SDK for Linux	Intel	31 OCT 2019			31 OCT 2019			(Simon Johnson)	
TCF	Intel	28 MAY 2020							
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	(Oct 2021?)	Vote in progress			FEB 2021
Keystone	UC Berkeley	23 JUL 2020	Yes	Yes	24 JUN 2021	MAR 2021		Stephen	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	Vote in progress		Zongmin	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021		Grant & Mike	APR 2021
CCC-Attestation	TAC	Yes	Yes	N/A	18 MAR 2021	18 MAR 2021		Dan & Aeva	(Veraison – OCT?)

CONFIDENTIAL COMPUTING CONSORTIUM

3. LPC Confidential Computing Microconference

- Linux Plumbers Conference 2021, Sept. 20-24, fully virtual

Confidential Computing MC

CFP Ends: TBD

The Confidential Computing microconference focuses on solutions to the development of using the state of the art encyption technologies for live encryption of data, and how to utilize the technologies from AMD (SEV), Intel (TDX), s390 and ARM Secure Virtualization for secure computation of VMs, containers and more.

Suggested Topics:

- Live Migration of Confidential VMs
- Lazy Memory Validation
- APIC emulation/interrupt management
- Debug Support for Confidential VMs
- Required Memory Management changes for memory validation
- Safe Kernel entry for TDX and SEV exceptions
- Requirements for Confidential Containers
- Trusted Device Drivers Framework and driver fuzzing
- Remote Attestation

For more references, see:

- AMD Secure Encrypted virtualzation
- Intel Trusted Domain Extensions
- ARMv9 Secure Virtualization

If you are interested in participating in this microconference and have topics to propose, please use the CfP process, and select "Confidential Computing MC" for the "Track". More topics will be added based on CfP for this microconference.

MC lead:

- Joerg Roedel <joro@8bytes.org>

CONFIDENTIAL COMPUTING CONSORTIUM

Open Source Summit North America, Sept. 27-30

- CCC now looking at pure virtual meetings
  - Plus in-person mostly unstaffed booth
- Sept 30 is not a normal TAC meeting week, Sept 23 would be
  - Kata containers now queued up to present at next meeting
  - Dave can't be there Sept 23 due to Linux Plumbers conflict (Jethro available to chair?)
  - Should TAC meet Sept 23 or Sept 30?
- Coordinated presence in kernel track regarding host-to-guest threat model?
  - https://github.com/confidential-computing/governance/issues/71
  - Do we need a technical whitepaper on the topic?
  - Attend LPC MC and look at whitepaper as follow-up

Some OSSNA Confidential Computing related talks

- **Monday**, September 27 • 2:30pm - 3:20pm
  - Using OP-TEE as a Cryptography Engine - Gregory Malysa, Timesys
- **Monday**, September 27 • 4:50pm - 5:40pm
  - Panel Discussion: Evolving the Confidential Computing Consortium: Non-profit Collaboration for Growth - Stephen Walli & Aeva Black, Microsoft; Mike Bursell, Congruus
- **Monday**, September 27 • 4:50pm - 5:40pm
  - Demystify Intel Security Technologies in the Firmware - Christian Walter, 9elements & Philipp Deppenwiese, immune GmbH
- **Tuesday**, September 28 • 5:25pm - 5:50pm
  - Panel Discussion: Experiences in Addressing Diversity, Equity, and Inclusion in Open Source Governance - Dan Middleton, Intel & Lindsay Nuon, EmpirEqual; Additional Panelists to be Announced
- **Wednesday**, September 29 • 11:30am - 12:20pm
  - OP-TEE: When Linux Loses Control - Clément Léger, Bootlin

CONFIDENTIAL COMPUTING CONSORTIUM

4. Updates from Outreach Committee

- Upcoming webinar topic ideas:
  - Sept. 23, afternoon Pacific time: IETF Remote Attestation Architecture – Dave T.
  - Nov 18?, Veraison – Thomas F.
  - Hacktoberfest? – Nick?
  - … TCG POV on CC? – Henk Birkholz? Etc…
- Status of Everest report – final by mid-sept?

5. Approval of TAC Minutes from July 1 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/07-Jul/CCC%20TAC%20Minutes%202021-07-01.pdf

RESOLVED: That the minutes of the July 1, 2021 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes from July 15 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/07-Jul/CCC%20TAC%20Minutes%202021-07-15.pdf

RESOLVED: That the minutes of the July 15, 2021 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes from August 26 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/08-Aug/TAC%20Minutes%202021-08-26.pdf

RESOLVED: That the minutes of the August 26, 2021 meeting of the Technical Advisory Council meeting of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

CONFIDENTIAL COMPUTING CONSORTIUM

VOTE: CCC Attestation SIG Chair - Ashley

- Proposed change of chair from Aeva to Larry Osterman

Diversity, Civility, & Inclusion policies

Add/update diversity and inclusion policies

- https://github.com/confidential-computing/governance/pull/83

Outreachy support

- https://www.outreachy.org/
- $6500 per intern
- Open source project responsible for mentor: https://www.outreachy.org/docs/internship/

- VOTE: Should the TAC fund an Outreachy intern for approved projects who want one?
  - Nick posted background to the list. We have a standing policy about Zoom, email lists, etc. If approved, this adds an Outreachy intern to the list of possible resources available from CCC funding.

- If yes:
  - Shall the TAC grant Enarx an Outreachy intern as requested?
  - Keystone? Veracruz?, Gramine?, Occlum?, OE SDK? – possible future period
  - Any project meeting the deadline

AWS Perspective on Confidential Computing - Mike

- https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective
- “We’ve observed that this phrase is being applied to various technologies that solve very different problems, leading to confusion about what it actually means. With the mission of innovating on behalf of our customers, we want to offer you our perspective on confidential computing.
- At AWS, we define confidential computing as **the use of specialized hardware and associated firmware to protect customer code and data during processing from outside access**. ...”

8. Any other business