Technical Advisory Council (TAC) Meeting

October 7, 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, Introduce any first-time attendees
2. Approval of minutes
3. Action item review
4. Gramine mentor
5. Tech Talk: Kata Containers
6. CCC security reports and VMT process
7. Updates from Outreach committee
8. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call, and Introductions

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*

2. Approval of TAC Minutes from Sept. 23 telechat

Thanks Jethro for chairing the meeting ☺

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/09-Sept/TAC%20Minutes%202021-23-09.pdf

RESOLVED: That the minutes of the Sept. 23, 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

3. Action Item Review

1. [Stephen] Chat with LF legal counsel to inform the process in place to establish a Vulnerability Management Team
2. [Ashley] Reach out to project mentors to confirm potential security contacts for each current and upcoming project
3. [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
4. [Thomas F.] Suggest changes on the White Paper in the shared Google doc
5. [Ashley] Reach out to Gramine for TAC presentation prior to board presentation
6. [Ashley] Invite Gramine for a board presentation after OSS (next virtual board meeting
7. [Thomas H/Eric V] Support text creation for VM terminology
8. [Dave/Ashley] Reach out to project mentors to schedule annual reviews for projects
9. [Ashley] Update CCC technical documentation to include internship policy as a project benefit

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?)	15 SEP 2021		Eric	FEB 2021 (DEC 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	15 SEP 2021		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 – NOV 18?)

4. Updates from Outreach Committee

5. LPC Confidential Computing MC follow-up

- Dave Thaler attended, anyone else?
- Guest-to-host threat model was discussed, general agreement among attendees on importance
- Some discussion of how to coordinate
  - https://github.com/confidential-computing/governance/issues/71
  - Some support for having discussion be coordinated or hosted (not discussed: mailing list? SIG?) by CCC, no other candidates mentioned

OSSNA Confidential Computing follow-up

- **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

6. TAC Tech Talks

Past TAC Talks (in addition to our own projects and proposed projects)

- IETF Remote Attestation -> Outreach webinar SEP 2021
- CNCF PARSEC
- Kata containers

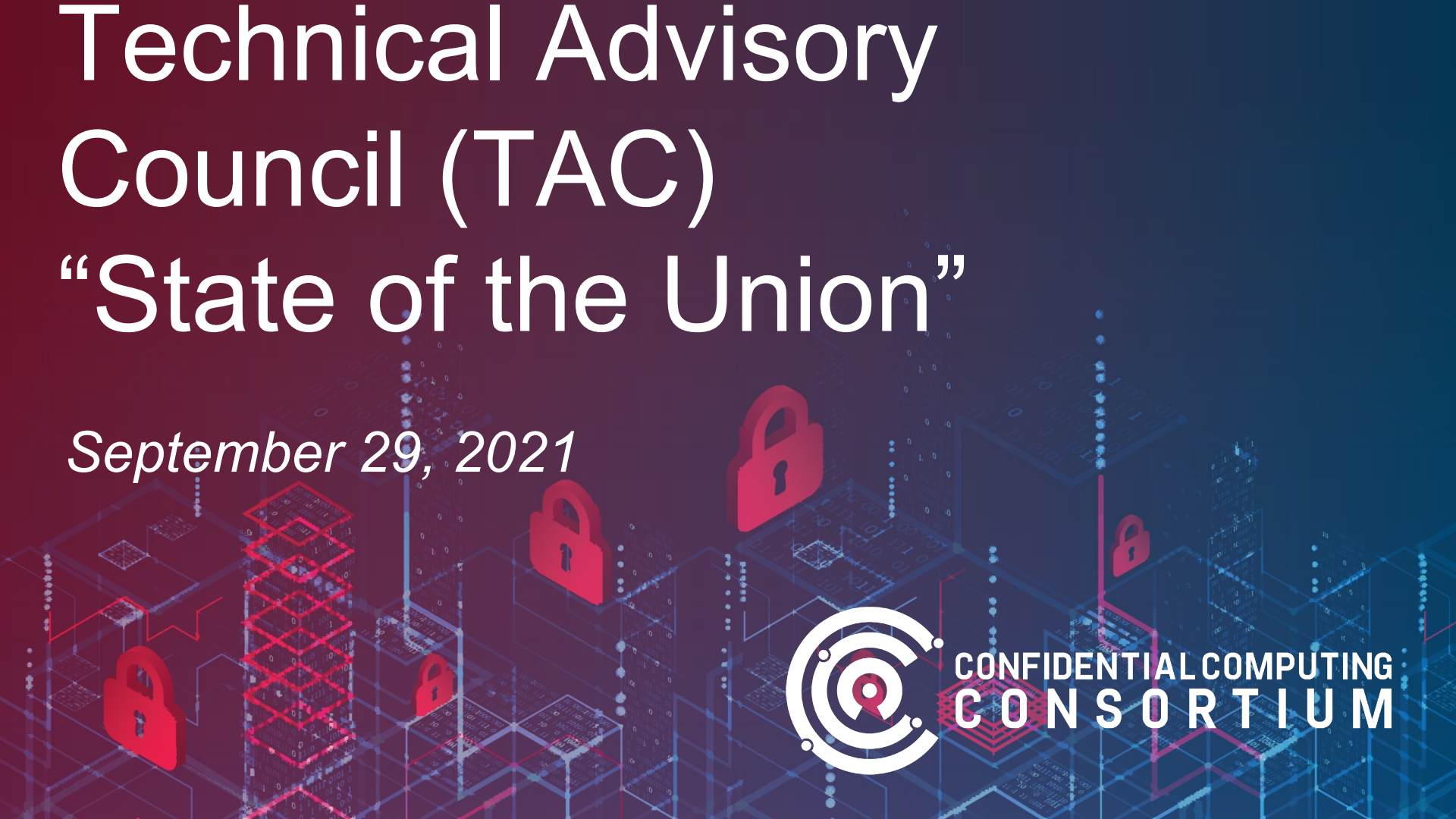
Any of the others candidates for a CCC webinar? How do we decide?

Possible TAC talks to solicit in future:

- TCG POV on CC? – Henk Birkholz?
- OP-TEE from TrustedFirmware.org
- Hacktoberfest? – Nick?
- Rust Hypervisor firmware: https://github.com/cloud-hypervisor/rust-hypervisor-firmware

Technical Advisory Council (TAC) "State of the Union"

September 29, 2021



Slide from Jan 2021
TAC report to Board

Areas of CCC Focus for Year #2

1. Cross-project coordination/communication
    - Cross-project chat (e.g., attestation channel)
2. Cross-org coordination
    - Standards orgs (IETF, GlobalPlatform, TCG, FIDO, HomomorphicEncryption.org, ...)
    - Government agencies (NIST, BSI, ...)
    - Open source orgs (CNCF, TrustedFirmware.org, Open Compute Project (OCP), …)
3. Additional collateral (whitepaper, terminology, talks)
4. Demos and tech talks in TAC meetings
5. Community development & DCI (diversity, civility, inclusion), see email thread

CONFIDENTIAL COMPUTING CONSORTIUM

We'll go through all those focus areas, as follows:

- Projects
- Security & vulnerability management
- Coordination with other technical bodies
- Whitepapers / technical collateral

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?)	15 SEP 2021		Eric	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	15 SEP 2021		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?)

Project benefits & expectations

- TAC Resources available to projects, on request
  - Zoom account
  - Outreachy intern
  - LF License Scanning
  - Email list hosting
  - …

- Added new expectations:
  - Clarified requirement to *have* a Code of Conduct to be submitted to CCC
  - Recommendation that maintainers/presenters take LF diversity training course
  - Incubation stage requirement to “Demonstrate that the project is invested in growing a diverse and inclusive community”

CCC security reports and VMT process

- Each Project is responsible for their own vulnerability management process
- Sometimes there are issues that affect multiple projects that need coordination across them
- TAC has a subteam working on a proposed mechanism here

Coordination with other technical bodies

- TAC talks, where we invite outside topics to be presented to the TAC
  - IETF Remote Attestation Procedures
  - CNCF: Platform AbstRaction for SECurity service (PARSEC)
  - Kata Containers
  - Upcoming: TCG
  - Upcoming: OP-TEE (from TrustedFirmware.org)
  - …
- Some TAC talks become recommended to Outreach as CCC webinar topics
  - IETF Remote Attestation Procedures this past month
- Have not yet had any related to governmental bodies, only standards bodies and open source bodies

CONFIDENTIAL COMPUTING CONSORTIUM

Whitepapers / technical collateral

- CCC FAQ updated
- Feedback received on technical whitepaper
  - TAC working on proposed updates to clarify technical questions raised
  - https://github.com/confidential-computing/governance/issues/77
- Also working on common terminology for “Confidential <X>”
  - Library, Process, Container, VM, …
  - Basic idea: confidential X means running X inside a hardware-based TEE
  - https://github.com/confidential-computing/governance/issues/79

CONFIDENTIAL COMPUTING CONSORTIUM

Questions?

- Any other requests to the TAC?

8. Annual Chair Election Timeline

- Last year's
  - TUE Nov 10, 2020: Call for nominations opens
  - TUE Nov 17, 2020: Call for nominations closes
  - WED Nov 18, 2020: Voting period opens
  - WED Nov 25, 2020: Voting period closes
  - TUE Dec 1, 2020: Election results announced
- Proposed timeline for this year:
  - TUE Nov 9, 2021: Call for nominations opens
  - TUE Nov 16, 2021: Call for nominations closes
  - WED Nov 17, 2021: Voting period opens
  - WED Nov 24, 2021: Voting period closes
  - TUE Nov 30, 2021: Election results announced

CONFIDENTIAL COMPUTING CONSORTIUM

9. CCC security reports and VMT process

- Gramine requested a mailing list for vulnerability disclosures across projects, internal to the CCC
- Existing VMT subteam to propose process: Aeva, Dan, Jethro, and Eric
- Subteam has been discussing offline, do we have a proposal for the TAC?

10. Establishing common terminology (issue #79)

Github Issue:

- https://github.com/confidential-computing/governance/issues/79

Doc in progress:

- https://docs.google.com/document/d/1xZ6IX0w0jaWDbLMFNAybTF3FpLnQ5TJ98nzIWbsbFnY/edit#

AWS Perspective on Confidential Computing

- 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**. ...”

11. Any other business