TAC Meeting

April 16, 2020

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 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. Approval of minutes
3. Action item review
4. Outreach report (Gartner debrief, Whitepaper status)
5. Review github issues & pull requests
    - #44: Updated IETF TEE definition
    - #41: Project progression template
    - #16: Project security response process
    - #17: Mapping “CCC project” to github terminology
    - #19: Project “charters”?
6. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call of TAC Voting Representatives

Quorum requires 5 or more voting reps:

Member	**Representative**	**Email**
Alibaba	Xiaoning Li	xiaoning.li@alibaba-inc.com
ARM	Grant Likely	grant.likely@arm.com
Facebook	Jinsong Yu	jinsongyu@fb.com
Google	Brandon Baker	bsb@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Simon Johnson	simon.p.johnson@intel.com
Microsoft	Dave Thaler(*)	dthaler@microsoft.com
Oracle	John Haxby	john.haxby@oracle.com
IBM/Red Hat	Mike Bursell - Dimitrios	mbursell@redhat.com

**TAC chair*

Approval of TAC Minutes from April 2 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2020/CCC%20TAC%20Minutes%202020-04-02.pdf

RESOLVED: That the minutes of the April 2, 2020 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

Action Item Review

1. [Mike/Aeva] Create the matrix for chat programs and send that to the list
2. [Stephano] Ensure that the Zoom links in the text files are merged with the invites. One link per group should make things a bit easier to follow. [MOSTLY DONE] link broken
3. [Stephano] Set up a Zoom account for OE SDK and work with Aeva on assigning a moderator
4. [Mike] Ensure that a TAC budget line item for 1 Zoom account for OE SDK
5. [Simon] Upload slides from Lyon, about the SGX SDK project

(other action items moved to github issues, listed later)

Gartner Analyst Meeting Debrief

- Attending – Brian Lowans, Tony Harvey. Then Ramon Krikken joined late, stayed late.
- Brian – what is your arrangement of service offering? Licensing?
- Ramon – What is your definition of TEE are you using?
- Brian – is post quantum included in this?
- Ramon – who is the audience for this?
- Ramon will read through slide deck. What is the probability AWS will join CCC?
- Document Review: He is happy to take a look at final draft of May 15 doc.
- Follow-ups:
    - Send TEE definition
    - Resend Presentation
    - Setup Document Review for Whitepaper

Other Outreach coordination items

- Please review whitepaper
  - [ref: Anne Bertucio Apr.14 email “Confidential computing whitepaper ready for input”]
- How can Outreach best coordinate with projects?
  - Projects (e.g., Graphene) need not be directly associated with members
  - TAC currently assigns mentor(s), should there be an Outreach-designated mentor? Or a project-specific contact for Outreach?
- Website: Outreach should manage all content?
  - Outreach is currently using google docs to edit and review
  - TAC is currently using Stephano’s github issues list to file issues
  - Should the github issues list be used?
  - Should all such issues be assigned to Outreach?

Pull Requests and issues

TAC issues have “TAC” label

Also experimenting with a Kanban project board to view status

Need more people’s github ids so can auto-add as reviewers

Issues at https://github.com/confidential-computing/governance/issues

- #16: Progression Template: Projects should address security response
- #17: Recommendations around mapping of "project" to github terminology
- #19: Project "charters"?

PR #44: Updated quote from IETF to match latest document

- IETF TEE Provisioning architecture draft had definition:
  - An environment that enforces that only authorized code can execute within that environment, and that any data used by such code cannot be read or tampered with by any code outside that environment.
- TAC provided feedback about “authorized” not being quite right
- New IETF text:
  - An environment that enforces that any code within that environment cannot be tampered with, and that any data used by such code cannot be read or tampered with by any code outside that environment.
- This matches the intent of the TAC slide on TEE properties (data integrity, data confidentiality, and code integrity)
- PR #44 updated the quote in the scoping.md document

#16: Project security response process

- TAC consensus for projects to have their own security process and roll up issues to the CCC TAC as needed
- More conversation is required around
    - Should CCC have a security committee, or only at the project level?
    - Should CCC have a security rep or advisor for projects?
    - If so, should that person be a TAC member or simply a security consultant?
    - Any best practice around embargos and embargo email lists? (i.e., who gets the notice of the embargo / vulnerability)

#17: Mapping “CCC project” to github terminology

- IF a project uses github… (not a requirement)
- Should it have its own GitHub organization, that can contain any number of repositories? (answer is already yes)
- Can new repos (or new code in same repo) increase the scope of the project beyond what was discussed in the original project submission?
- Propose:
  - Annual Project Review should check whether the answers in the submission template are still correct or need to be changed
  - Projects should be encouraged to proactively inform the TAC when something changes that affects their submission template (changing a License, security reporting process, CoC, etc.).

#19: Project “charters”?

- Our “Project Progression Policy” currently says:
  - The proposal document will be finalized and a project charter prepared. This charter document must be included in the project's main repository.
- Do we actually want this, or remove this text?
- What is the project "charter"?
- Who creates it, the TAC or the project's own governance?
- Who is authoritative for its contents?
- Is there a charter template, or any examples of such a "charter" to point to?

Any other business

* Alternate voting members