TAC Meeting

May 14, 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. Chat service – Mike/Aeva
5. Outreach-related topics
    - Project contacts
6. Threat Model slides and future whitepaper – Brandon/Mike
7. Time permitting:
    1. Issue #16: Security response process
    2. PR #42: TEE attributes document
    3. PR #46: Progression policy update
8. Any other business

CONFIDENTIAL COMPUTING CONSORTIUM

Roll Call of TAC Voting Representatives

Quorum requires 5 or more voting reps:

Member	Representative	Email
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
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
Red Hat	Mike Bursell	mbursell@redhat.com

**TAC chair*

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes from April 30 telechat

https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2020/04-Apr/CCC%20TAC%20Minutes%202020-04-30.pdf

RESOLVED: That the minutes of the April 30, 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] Set up a Zoom account for OE SDK and work with Aeva on assigning a moderator
3. [Mike] Ensure that a TAC budget line item for 1 Zoom account for OE SDK
4. [Simon] Upload slides from Lyon, about the SGX SDK project
5. [Xiaoning, Jinsong, ~~Brandon~~, Howard, John, & Giuseppe] Send Dave or Stephano your GitHub ID so that we can add reviewers to our GitHub issues / pull requests

(other action items moved to github issues)

Chat: questions to consider

- should the CCC
  - fund chat services for projects?
  - host chat services for projects?
- should all projects use the same chat services?

Project contacts

- 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?

Confidential Computing Threats Mitigated and Security Research

Mike Bursell (Red Hat)
Brandon Baker (Google)

CONFIDENTIAL COMPUTING CONSORTIUM

CCC Threat Model

Goal

Confidential Computing aims to reduce the ability for the owner/operator/pwner of a platform to access data and code inside TEEs sufficiently such that this path is not an economically or logically viable attack.

Threat vectors

- Software attacks
  - Host operating system, hypervisor, BIOS, and other software/workloads
- Basic physical attacks
  - Cold DRAM extraction, bus and cache monitoring
  - Plugging in an attack device to an existing port, e.g. PCIe, Firewire, USB-C

CCC Threat Model

Out of scope

- Sophisticated hardware attacks
  - Chip scraping
  - Electron microscope probes
- Upstream supply-chain attacks
  - At chip manufacturing time
  - At key injection/generation time

- Different TEE implementations will have varying degrees of resistance to cryptographic attack.
  - Particularly true of integrity attacks, rollback, and replay

Time Permitting

Side Channels

- Novel attack chain. Significant area of research
- Some side channels considered out-of-scope by hardware vendors
- Limited utility in the wild, not seeing them in practical use
- Successful exploitation requires quiet host environment, long-term noisy access
- Targeting and colocation on Cloud platforms is challenging
- Industry is working to address them, both in software/microcode and in subsequent hardware generations

- Attestation of platform configuration, microcode version necessary

Issue #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)
  - What is the criteria to get on the list of who gets the private notices and is it documented?

Issue #36: What if a project wants to spin-off a library as sub-project?

- Simon asks: “Do we need any specific process for spinning-out a sub-project from an already approved project? Or does it become just another a second project under the auspices of previously approved project?”
- Suggested answer:
  - CCC project can have any number of repos under same github org (if using github)
  - If intent is to still be part of same CCC project as far as website, etc goes:
    - No specific process, project can just move code to another repo under same github org
  - Else if intent is to be viewed as a separate (new) CCC project:
    - Would need to go through TAC review as any other new project would

Any other business

[Simon] scheduling a project proposal review for the following TAC meeting