TAC Meeting

March 5, 2020

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.

Agenda

1. Roll call
2. Approval of minutes
3. Action item review
4. Additional TAC materials for analyst meeting
   a) TEE definition
   b) Relationship to other related technologies (HE, TPM, ...)
5. Future TAC work
   a) Whitepaper on various types of TEEs
   b) Use cases
6. Any other business

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
Red Hat	Mike Bursell	mbursell@redhat.com

**TAC chair*

Approval of TAC/Outreach Joint Meeting Minutes

https://lists.confidentialcomputing.io/g/main/files/F2F/2020%20-%20RSA/CCC%20Outreach%20Minutes%202020-02-27.docx

RESOLVED: That the minutes of the February 27, 2020 **joint** meeting of the Technical Advisory Council and Outreach Committee of the Confidential Computing Consortium as distributed to the members of the TAC in advance of this meeting are hereby adopted and approved.

Approval of TAC Minutes

https://lists.confidentialcomputing.io/g/main/files/F2F/2020%20-%20RSA/CCC%20TAC%20Minutes%202020-02-27.docx

RESOLVED: That the minutes of the February 27, 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.

Action Item Review

1. [Stephano] Eventually provide a better way (wiki list, perhaps GitHub issues) to track website content requests and their progress.
2. [Stephano] Make meeting recordings be discoverable in Groups.io in the TAC group only
3. ~~[Pushkar Chitnis] Provide details for OE SDK ask on CI/CD pipeline costs [DONE]~~
4. ~~[Stephano] Move outreach files into the main group and send a link to the list so that the TAC can access their materials (specifically the Positioning) [DONE in joint meeting minutes]~~
5. [Stephano] Add boilerplate templates to the “files” area of main group [DONE]
6. [Stephano] Find the mission statement and submit a pull request for adding it to our GitHub repo
7. [Stephano] Create a document around GitHub process and propose at the next conference call
8. [Simon] Propose a list of project categories for discussion

Analyst Briefing Prep

Outline

- Introductions and Agenda – Seth (10 minutes)
- Confidential Computing Consortium Mission – Stephen (10 minutes)
- **Definition and Characteristics of Confidential Computing – Dave Thaler (10 minutes)**
  - **Definition, Characteristics, Advantages relative to adjacent technologies**
- **Threats Mitigated and Security Research – Mike/Brandon (10 minutes)**
  - **Explain the threats Confidential Computing protects against and address side-channel attacks**
- **Current State of Public Cloud Confidential Computing Adoption – Aeva (10 minutes)**
- Customer Traction and Use Cases – Nelly/Morgan (10)

Scoping: TAC Recommendations

- The TAC recommends that the scope of the consortium be to "promote the widespread use of **hardware-based trusted execution environments**".
- The TAC recommends that the definition of the term Confidential Computing be: "Confidential Computing is the protection of data in use by performing computation in a **hardware-based Trusted Execution Environment**.“
- For both the scope of the CCC, and the definition of confidential computing, the TAC recommends avoiding using the following terms in ways that imply constraints, as being technically problematic: "cloud", "main processor", and "encrypted"/"encryption".
- Similarly, the TAC recommends against any language implying that "protecting data in use" is synonymous with "confidential computing", as the latter is only a subset of technologies for the former.

Do we need to define “hardware-based TEE”?

TEE definitions from previous discussion:

- An environment that enforces that only authorized code can execute with that environment, and that any data used by such code cannot be read or tampered with by any code outside that environment. [IETF]
    - Simon had some issue with “authorized”?
    - Definition is for a “TEE” not a “hardware-based” TEE
- A hardware-based technique for securing sensitive data and algorithms in such a way that even the kernel, root user or hypervisor can't see what's going on. [other strawman discussed]
    - But “a processor (e.g., an MCU) might *only* have a TEE and no REE”

But what is a “hardware-based TEE”?

Required properties to be called a “TEE”:

- **Data integrity**
- **Data confidentiality**
- **Code integrity**: *was* “algorithmic (mathematical) vs hardware/software”

Other properties that not all TEEs have, or at least not to the same degree:

- Code confidentiality
- Programmability: *was* “generalised vs specialised computation only”
- Authenticated “boot” (aka secure boot)
- Unspoofability (un-clonable identity) / non-repudiability (identity tied to a transaction)
- Attestability of platform/stack
- Recoverability

Security Comparison vs Related Technologies

Feature	Technology		
	HW TEE (e.g., SGX)	Homomorphic Encryption	Secure Element (e.g., TPM)
Data integrity	Y	Y (subject to code integrity)	Keys only
Data confidentiality	Y (if side-channel attacks prevented)	Y	Keys only
Code integrity	Y	No	Y
Code confidentiality	Y (with work)	No	Y
Programmability	Y	Partial (“circuits”)	No
Unspoofability/Recoverability	Y	No	Y
Attestability	Y	No	Y

Technologies can be combined to get even better security

Scalability Comparison vs Related Technologies

- Scalability across data sets (Ability to combine data - MPC)
  - Native == TEE > HE
- Data size limits: Native > TEE > HE
- Computation speed: Native > TEE > HE
  - (idea: use a spectrum where native/tee are close and HE is farther to the right)

Combining (TEE+HE) generally means lower scalability

Ability to scale out: doable with HE, maybe doable with TEE in future with framework work?

Future TAC work

Future TAC Documents?

- CC use cases: Simon, Morgan, … (end user forum)
    - Some being prepared by Outreach for analyst briefing
- Whitepaper on various types of TEEs? Dave, Simon, …
    - Should Seth ask Outreach whether this is needed/useful?
    - Generics or also vendor-specific info? Leave vendor info to vendor sites
- …

Volunteers?

Any other business