DRAFT

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Conference Call – 7:00am PST
Thursday 5 March 2020

1. Call to Order / Roll Call

- a. Members of the Technical Advisory Council
  - i. Dave Thaler (Microsoft) (Chair) *
  - ii. Aeva van der Veen (Microsoft)
  - iii. Grant Likely (Arm)*
  - iv. Simon Johnson (Intel)*
  - v. Simon Leet (Microsoft)
  - vi. Seth Knox (Outreach chair)
  - vii. David Dunn (VMware)
  - viii. Morgan Akers (JPMC)
  - ix. Ahmad Atamlh (Mellanox)
  - x. Jethro Beekman (Fortanix)
  - xi. Ahmad Atamlh (Mellanox)
  - xii. Lei Zhang (iExec)
  - xiii. Wenjing Chu (Futurewei)*
  - xiv. Brandon Baker (Google)*
  - xv. Naveen Cherukuri (Nvidia)
  - xvi. John Haxby (Oracle)*
  - xvii. Howard Huang – (Huawei)*
  - xviii. Gorav Arora (Thales Group)
  - xix. Stephano Cetola (Linux Foundation)
- b. Not in attendance
  - i. Mike Bursell (Red Hat)*
  - ii. Xiaoning Li – (Alibaba)*
  - iii. Faiyaz Shahpurwala (Fortanix)
  - iv. Richard Searle (Fortanix)
  - v. Jinsong Yu (Facebook)* *voting member

2. Move to approve minutes

- a. The committee defers approval the minutes for the February 27, 2019 meetings, both the joint meeting and the non-joint meeting.

3. Action Item Review

- a. [Stephano] Find a way to track website changes, create a document regarding how we use GitHub, make recordings available on the TAC Groups.io section that makes sense. [In Progress]
- b. [Simon] Propose a list of project categories for discussion. [In Progress]
- c. [Mike Bursell] Work with the LF (and possibly RH) to see how we should, as a group, work cross-project on things like SRT bugs, disclosures, embargos, etc. [In Progress]

4. Do we need to define "hardware-based TEE"?

a. There is an IETF definition, however it has been noted that “authorization” is not a necessary part of a definition for us. There is a distinction between “measured boot” and “authenticated boot”.

b. There is another strawman definition that was also proposed, but that brought up the question of what properties are required to call something a TEE. Perhaps those properties are what is important to list, rather than a definition. The following properties were proposed:
   i. Data integrity
   ii. Data confidentiality
   iii. Code integrity
   iv. Code confidentiality
   v. Programmability
   vi. Unspoofability / Recoverability (un-cloneable identity)
   vii. Attestability
   viii. Authenticated “boot” (aka secure boot)

5. **Scalability Comparison vs Related Technology**
   a. Dave is preparing for 10 min discussion here for analysts. HW Tee, Homomorphic Encryption, and TPMs were compared and contrasted. Main topics he will discuss include scalability across datasets, data size limits, and computational speed.
6. **Public Cloud Adoption and Projects (probably 2 slides)**
   a. Inverted pyramid to represent folks not currently in our graduation ladder
      i. Hardware at the bottom
      ii. Cloud providers in the center
      iii. ISVs at the top
   b. Regular pyramid showing maturation
      i. Bottom - the sandbox (including CCC and non-CCC members)
      ii. Middle - incubation level (customer adoption, but not stable commitments)
      iii. Graduation phase (Fortanix has examples, discuss via email)
   c. Keeping products and OS projects separate is key here
7. **Preliminary Ideas – Threats Mitigated and Security Research**
   a. Technology is new an evolving, different forms protect against different threats, this is one of the goals of the CCC is to help folks understand which threats map to TEEs.
   b. Cloud provider use case: CC limits, reduces, or eliminates the risk of running software on a machine where customer code or data is put at risk.
   c. Hardware attacks: CC (TEE) may be useful in mitigating certain attacks (e.g. plugging in devices, freezing and walking off with DRAM chips). The basic physical attacks are valuable to discuss, rather than more complex physical attacks.
   d. Attacks on supply chain: related to some of the more complex or advanced physical attacks.
   e. Keep in mind that all mitigations are subject to errors of implementation either in hardware or software. We want to be careful not to present this as a silver bullet of any kind.
   f. Edge / IoT use cases: E.g. Manufacturer has a ML model that is in their device. That model is the thing they want to keep confidential. CC allows them to ship that device without the threat of someone getting access to that model. Protection of medical equipment where the patient’s confidential health data is collected on the device.
8. **Future TAC Documents**

a. Confidential Computing Use Cases
  i. TAC Should drive what these use cases are while Outreach can bring ideas to the TAC.
  ii. Use cases help drive projects that we might be interested in.
  iii. They also help communicate the value of the CCC in general, so having a standard set that we can reference in any content we produce would be ideal.

b. Whitepaper on various types of TEEs
  i. The Outreach committee has discussed this, and Seth believes that we need this sort of document.
  ii. It should encompass a more detailed definition than the analyst briefing, it should cover generics but not vendor specific details. Dave will work on this, possibly with help from Simon and Mike (assuming he volunteers). Pull requests are as always open to all.

9. GitHub Issues Discussion

a. #14 – Should we have any guidance on what Code of Conduct is acceptable
  i. Is the policy around the CoC a TAC issue, or is that the board or legal group's purview? The TAC requires that each project has a CoC, but the board should agree that the CoC the project adopts is adequate. We will continue discussion.
  ii. https://www.contributor-covenant.org/
  iii. https://github.com/confidential-computing/governance/issues/14
  iv. The TAC got consensus to recommend projects use Contributor Covenant v2.0 as a baseline, but if projects want to diverge, that would be allowed (and lightly discussed).
    1. https://www.contributor-covenant.org/version/2/0/code_of_conduct/

Action Items

1) [Simon] Start a list of use cases to help Outreach develop content and clarify which projects we might want to work with. Please reach out to Morgan for brainstorming.
2) [Dave] Work with Simon (and Mike?) on the whitepaper text.

Meeting adjourned at 9:01 am PST on March 5, 2020. The next conference call will be scheduled for Thursday March 19th.

Respectfully submitted by Stephano Cetola, Acting Secretary, on March 6, 2020.