DRAFT

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Conference Call – 7:00am PST
Thursday 15 October 2020

1. **Call to Order / Roll Call**

   1.1. **In Attendance**

      1.1.1. Dave Thaler (Microsoft, TAC Chair) *
      1.1.2. Aeva Black (Microsoft)
      1.1.3. Brandon Baker (Google)
      1.1.4. Dan Middleton (Intel)
      1.1.5. Dimitrios Pendarakis (IBM) *
      1.1.6. FX Marseille (Thales)
      1.1.7. Giuseppe Giordano (Accenture) *
      1.1.8. Hannes Tschofenig (Arm)
      1.1.9. Jethro Beekman (Fortanix)
      1.1.10. Liam Coffey (AMD)
      1.1.11. Michael Lu (Arm)*
      1.1.12. Naveen Cherukuri (NVIDIA)
      1.1.13. Roy Hopkins (R3)
      1.1.14. Seth Knox (Outreach Chair)
      1.1.15. Shankaran (Facebook) *
      1.1.16. Simon Johnson (Intel) *
      1.1.17. Simon Leet (Microsoft)
      1.1.18. Stephen Walli (Microsoft)
      1.1.19. Xinxin Fan (IoTex)
      1.1.20. Stephano Cetola (Linux Foundation)

   1.2. *voting member

2. **Move to approve minutes**

   2.1. The Technical Advisory Council approves the minutes from the September 17 meeting with no abstentions and no objections.

   2.2. The Technical Advisory Council approves the minutes from the October 1 meeting with no abstentions and no objections.

3. **Action Item Review**

   1. [Mike] Ensure that a TAC budget line item for 1 Zoom account for OE SDK
   2. [David Kohlbrenner/Stephano to remind] Please provide a list of the licenses used by Keystone for crypto implementations, specifically to ensure that they are all OSI approved.
   3. [Stephano] Ping Mike if we can’t redirect Enarx mailing list [In Process]
   4. [Stephano] Work with the Occlum folks to get a list of the dependencies listed which are part of the TCB and add that to the submission document for posterity [DONE]
   5. [Aeva/Mike] Create straw-person for terminology proposal [In Process]
   6. [Dave] Update the Project Progression Policy to match the board charter change regarding Graduation stage projects and voting [In Process]
   7. [Stephen] Please reach out to Cat Allman regarding any details we can get on LISA21. [In Process]

8. [Stephano] Get the timing diagram graphic to LF Creative so that we can review it. [DONE]
9. [Stephano] Set up a vote for a chat system, ~~pinging the LF to ensure that Slack is still the default / most popular choice~~. [In Process]

4. **CCC & CNCF SIG-Security - Aeva**

4.1. There is a rough list of about 7 projects in the CNCF that are currently looking at Confidential Computing as part of their use cases.

4.2. This was an initial meeting, an overview and introduction for the CCC, where we discussed how we work better cross-organizationally.

4.3. These CNCF SIG Security meetings are open to all:

4.3.1. https://github.com/cncf/sig-security

4.4. More updates after late November, once Kubecon has passed. Getting our projects talked about in a large org like CNCF is a great was to make our work more visible.

5. **Interop Working Group Proposal (Gilad Golan)**

5.1. Investigate and promote industry standards:

5.1.1. Authentication of CC environments (attestation)

5.1.2. Secure communication with and among CC environments

5.1.3. Secure sealing of secrets to CC environments

5.2. Proposal: Interoperability Working Groups or SIGs

5.3. The question of should this be restricted to attestation, or do we want it to cover a broader range of topics with this group?

5.4. Also, there exists an attestation mailing list, so the question was raised if we should simply reuse this list or does this need to be a separate effort?

5.5. Attestation Mailing List reminder: https://lists.confidentialcomputing.io/g/attestation

5.6. All projects are welcome to join in on any conversation regarding attestation on this list. This is not specifically for the whitepaper but rather for general conversation.

5.7. Brandon will provide a document for folks to review that will go into more detail on the formalization of this working group, define scope, output criteria, goals, and to provide some accountability to the TAC about the output.

5.8. One of the goals of the working group would be to look at standards like IETF RATS and would be scoped narrowly to interoperability in terms of attestation only.

5.9. More info coming on the ML and discussions at the next TAC meeting.

6. **TAC Whitepaper**

6.1. [Thomas] You suggested adding a sentence in the Introduction section about the intended audience, perhaps simply changing the last sentence. Any guidance here appreciated. This action item is a reminder to follow up on this in the next meeting.

6.2. ~~[Mike] Please clarify the section 6.2.1 “Threat Vectors -> In-Scope” regarding crypto in hardware vs crypto in firmware/software.~~

6.3. ~~[Michael] Please have an Arm attestation lead review the document before October 15.~~

6.4. Discussion around updates to the documents. Highlights include creating a versioning scheme, ensuring the references are up to date, and creating a document title.

6.5. Current working title: **Confidential Computing Deep Dive**

6.6. Examples of how we might do change tracking:

6.6.1. https://www.intel.com/content/dam/www/public/us/en/documents/reference-guides/pcie-device-security-enhancements.pdf

6.6.2. https://trustedcomputinggroup.org/wp-content/uploads/Errata_v1p1_for_TPM2p0_Library_Spec_v1p59_pub.pdf

6.7. We will make the scoping document look similar to the TAC whitepaper once the changes to scoping are accepted on Github. This may happen after the conference depending on timing.

6.8. For a Venn diagram we chose option A for this version: https://lists.confidentialcomputing.io/g/tac/files/ccc-venn-diagram-v1.pdf

7. Areas of CCC Focus for Year #2

7.1. Cross project chat is in progress. Voting on a platform coming soon.

7.2. Cross Org Coordination

7.2.1. Standards orgs (IETF, GlobalPlatform, FIDO, etc)

7.2.2. Government Agencies (NIST, BSI, etc) – NIST is having a panel discussion on the Oct 22, Dave will be a panelist: https://www.nist.gov/news-events/events/2020/10/workshop-cybersecurity-risks-consumer-home-iot-products

7.2.3. Open Source Orgs (CNCF, TrustedFirmware.org, Open Compute Project (OCP), etc)

7.2.4. Demos & Tech Talks

7.2.5. Community Development and Diversity & Inclusion

7.3. Additional Collateral (Whitepapers, Conference Talks, Terminology)

7.4. Demos and tech talks

8. Pull Requests

8.1. https://github.com/confidential-computing/governance/pulls

8.2. Please check #66 and #62 as they currently require TAC review. Specifically, #62 should be ready to review, and we'd like to have that for the October 26 OSS EU deadline. These both have the timebomb tag on them.

8.3. Also a note on issue #50 as this will be a future action item for this group.

9. Next Meeting

9.1. Oct 26 is OSS

9.2. Oct 29 is the next TAC

Action Items

1. [Seth/Stephano] Discuss how to properly version the whitepaper with the Outreach committee and ensure that the links from the TAC whitepaper point to the latest version.

1.1. Two examples we might consider, #1 and #2.

2. [Brandon] Provide a document for TAC review detailing the formalization of an interop working group: define scope, output criteria, goals, and to provide some accountability to the TAC about the output.

Meeting adjourned at 9:06 am PT on October 15, 2020. The next conference call will be scheduled for Thursday October 29.

Respectfully submitted by Stephano Cetola, Acting Secretary, on October 19, 2020.