DRAFT

TAC Conference Call – 7:00am PST
Thursday 16 December 2021

1. **Call to Order / Roll Call**
   - Ashley Weltz (Linux Foundation)
   - Dave Thaler (Microsoft, TAC Chair)*
   - Brian Warner (Linux Foundation)
   - Eric Voit (Cisco)
   - Nick Vidal (Enarx)
   - Jethro Beekman (Fortanix)
   - Simon Johnson (Intel)
   - Shalom Shefa (Cisco)
   - Zhipeng Huang (Huawei)*
   - Thomas Fossati (Arm)*
   - Naveen Cherukuri (NVIDIA)
   - Wojtek Porczyk (Gramine)
   - Borys Poplawski (Gramine)
   - Ran Lifshitz (HUB Security)
   - Eric Northup (Meta)
   - Samuel Ortiz (Kata Containers)
   - Penglin Yang (Enarx)
   - Steve Van Lare (Anjuna)
   - Lily Sturmann (Red Hat)*
   - Dmitrii Kuvaiskii (Gramine)
   - Dimitrios Pendarakis (IBM)
   - Nathaniel McCallum (Profian)
   - Mona Vij (Gramine)

     *voting member

2. **Move to approve minutes**
   2.1. The Technical Advisory Council has already approved the minutes from the December 2nd meeting. The minutes from the November 18th meeting have been tabled for review and approval at the January 12, 2022 meeting.

3. **Action Item Review**
   3.1. **[Mike, Eric, Stephen, Zongmin, Grant/Mike, Dan/Aeva]** Recommend diversity and inclusion training to their projects and report back to the TAC on whether the maintainers or the contributors will be taking it and when the expected completion date is. **[IN PROGRESS]**
   3.2. **[Dave]** Coordinate with the organizer from LPC microconference about linux-colllab list. **[DONE]**
   3.3. **[VMT Subteam]** Meet with Stephen to identify the process for establishing VMT.
      3.3.1. VMT is meant to help unwind unclear dependencies.

3.3.2. CCC uses minimum viable governance. In this spirit the best path forward is to have each project self-report their dependencies and have a central list for notifications with reps from each project.
3.3.3. Discussion ensued over the Xen Project processes for VMT.
3.3.4. Need to clarify what can and cannot be disclosed during embargoes.
3.3.5. Discussion ensued over keeping the dependency checklists up to date to assess the scope of embargoes.
3.3.6. How will the cross-project security list be used?
3.3.6.1. Primary reporting is to an individual project's reporting mechanism
3.3.6.2. Use the proposed CCC report address, if a vulnerability applies to multiple projects or the affected projects are unknown.
3.3.6.3. If a project receives a report that may also apply to other projects that project can coordinate with the other projects or use the central list.
3.3.7. Discussion ensued over MOUs vs. NDAs.
3.3.7.1. Projects can't sign NDAs.
3.3.7.2. MOUs may be an option in some circumstances.
3.3.8. Reports will likely be in a few common categories: vulns that go across multiple projects (hardware or crypto library)
3.3.9. Next steps
3.3.9.1. Examples of embargo: Xen Project (fix distribution without disclosure) https://xenproject.org/developers/security-policy/
3.3.9.2. Notice to projects that their security contact emails will be aggregated into a centralized list.
3.3.9.3. Consider adding the central policy / reporting steps to https://github.com/confidential-computing/governance/blob/main/security-response-policies.md which is currently just project responsibilities.
3.4. [Dan] Provide contact for Rust Hypervisor firmware.
3.5. [ALL] Review, comment and/or correct text in Common Terminology Document: https://docs.google.com/document/d/1xZ6IX0w0jaWDbLMFNAybTF3FpLnQ5TJ98nzIWbsbFnY/edit [IN PROGRESS]
3.6. [Ashley] Add recording link to the bottom of the minutes moving forward. [DONE]
3.7. **[Ashley]** Add new Occlum dependencies to spreadsheet https://docs.google.com/spreadsheets/d/1UKnbbGWXYLjnPZsox3zmYo59nv3XSXjePfas5E2fER0/edit#gid=0 **[DONE]**

4. Updates from Outreach Committee
4.1. Aeva shared a recap from RISC-V Summit via the Outreach mailing list.
4.2. If you are attending RSA in person, please notify Ashley of your attendance.

5. Establishing Common Terminology
5.1. Discussion continued on comments and edits made to the Establishing Common Terminology document.
5.2. Discussion ensued around if we need all of the definitions listed or if defining a sub set of them would be sufficient.
5.3. A call to action was made for anyone who had edits or suggestions to the document to add a comment with their thoughts.
5.4. Github Issue:

5.4.1. https://github.com/confidential-computing/governance/issues/79
5.5. Doc in progress:
5.5.1. https://docs.google.com/document/d/1xZ6IX0w0jaWDbLMFNAybTF3FpLnQ5TJ98nzIWbsbFnY/edit#
5.6. Anjuna's slides
5.6.1. https://lists.confidentialcomputing.io/g/main/files/TAC/Meetings/2021/11-Nov/AnjunaDefinitions.pdf

6. **Approving Hardware Requests**
6.1. Enarx submitted a written proposal via email in request for hardware.
6.2. The group discussed the procedure for projects requesting hardware within the already approved policy.
6.3. A vote will not need to be made to move forward with requests. Projects will be asked to bring their request to the TAC.
6.4. A decision still needs to be made on whether the project orders the hardware and is reimbursed or the TAC places the order on behalf of the project.
7. **Any other Business**
7.1. Keystone's annual project review and the Homomorphic Encryption Tech Talk with Rosario Cammarota will take place on January 13, 2022.
7.2. Veraison new project submission and OP-TEE with Julian Hall will take place on January 27, 2022.

Action Items:
[Nathaniel] Identify a definition that Enarx can fit into on the Common Terminology document and define what is the smallest unit (such as a confidential computation).
[Steve] Define a term that is wider than only protecting data.

Recording:
https://zoom.us/rec/share/_LRCvPH-k017INuzDiEnmCgCnn003p1NXOm-3KUC4gVb92_SCRr-FjeA40rs-9A_.nSvosnVZ_wOdKnjT

Meeting adjourned at 9:00am PST on December 16, 2021. The next conference call is scheduled for Thursday January 13, 2021 at 7am PST.