DRAFT

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Conference Call – 7:00am PST
Thursday 23 July 2020

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

 1.1. **In Attendance**

  1.1.1. Dave Thaler (Microsoft) (Chair) *
  1.1.2. Seth Knox (Outreach Chair)
  1.1.3. David Kohlbrenner (UC Berkeley / UW)
  1.1.4. Aeva Black (Microsoft)
  1.1.5. Xinxin Fan (IoTex)
  1.1.6. Shankaran (Facebook)*
  1.1.7. Simon Leet (Microsoft)
  1.1.8. Dimitrios Pendarakis (IBM)*
  1.1.9. Roy Hopkins (R3)
  1.1.10. Jethro Beekman (Fortanix)
  1.1.11. Naveen Cherukuri (Nvidia)
  1.1.12. Grant Likely (Arm)*
  1.1.13. Liam Coffey (AMD)
  1.1.14. Giuseppe Giordano (Accenture)
  1.1.15. Michael Lu (Arm)*
  1.1.16. Francois Xavier (Thales)
  1.1.17. Richard Searle (Fortanix)
  1.1.18. Michael Klein (Accenture)
  1.1.19. John Haxby (Oracle)
  1.1.20. Xinxin Fan (IoTeX)
  1.1.21. Ry Jones (Linux Foundation / Hyperledger)
  1.1.22. Stephano Cetola (Linux Foundation)

 1.2. *voting member

2. **Move to approve minutes**

 2.1. The committee approved the minutes for the July 9 meeting with no objections and one abstention.

3. **Action Item Review**

 3.1. [Mike] Ensure that a TAC budget line item for 1 Zoom account for OE SDK
 3.2. [Xiaoning] Send Dave or Stephano your GitHub ID so that we can add reviewers to our GitHub issues / pull requests
 3.3. [Mike/Brandon/Simon/Jethro] Continue to create text for an in-depth TAC whitepaper (ON AGENDA)
 3.4. [Mike/Richard] For the Chat Comparison spreadsheet, define some of the comparison items that might be confusing in a markdown document in the GitHub repo
 3.5. [Stephano] Survey for health check across members, starting from sample questions in July 9 TAC minutes. And include Outreach and Board. [In Process]
 3.6. [Dave] Reference new Steve Riley Gartner TEE definition in TAC Scoping.

4. **Keystone TEE Framework Overview**

 4.1. Keystone is an alternative way to build TEE themselves.

4.2. Targeting RISC-V, we allow folks to take a piece of RISC-V hardware, use our software to turn that into a TEE supporting platform. The only requirement is a key (locked down) that comes from the manufacturer.

4.3. Keystone allows us to make performance / security tradeoffs. Keystone can decide which security features are available when constructing the "Security Monitor".

4.4. This aligns very well with the Consortium's mission, and we hope to integrate with Open Enclave SDK, so we see a lot of natural partnerships there.

4.5. For more information, see the submission template:

4.5.1. https://lists.confidentialcomputing.io/g/main/files/TAC/Project%20Submissions/Submitted/Keystone-CCC-Application.pdf

4.5.2. https://github.com/keystone-enclave

5. Keystone TEE Framework TAC Questions

5.1. Which Crypto Algorithms do you implement?

5.1.1. Keystone implements SHA256 and some ECC implementations. Those were added early on and are not core to the Keystone system. We are looking to improve how we currently hash (measure) our enclaves initially (on creation).

5.1.2. For applications we use libsodium, for the security monitor we use independent implementations that we would like to replace for build reasons.

5.1.3. David can provide a list of licenses for these library implementations to ensure they are all on the OSI approved list.

5.2. How do you differentiate yourself from a Type-1 Hypervisors?

5.2.1. A type-1 hypervisor can run on top of Keystone. We are not doing any kind of resource allocation or scheduling. Our Security Monitor does not have a concept of virtual memory, managing page tables, but rather operates on physical memory.

5.3. What does the TEE provide in terms of services?

5.3.1. Each enclave consists of a user and supervisor (kernel) component (see 2.2.1). A runtime can be a full microkernel or a few hundred lines of shim code.

5.4. Is there anything you'd add to our definition of a TEE (in the TAC whitepaper)?

5.4.1. Potentially additional features that require hardware support. A good example of this on a base RISC-V platform, do not provide protection against cache side channels. However, on a platform we have used for much of our development, it has a configurable cache controller, and we have built modules that can be built for that TEE (if you're using that hardware) that allow applications to ask for transparent cache partitioning.

5.4.2. Right now we do not have a authenticated launch mechanism. The Security Monitor is easily modified and updated, so someone could easily build on top of that.

5.5. How do you compare to something like Trusted Firmware or OP-TEE?

5.5.1. The advantage of building on top of RISC-V (from our perspective) we have a better core primitive, the Physical Memory Protection (PMP) mechanism. From that simple primitive base, we can build a smaller thinner baseline that allows us to have a wider set of TEE models that protect against different sets of threat models.

5.6. Attestation – see here for an overview

5.6.1. We have a simple attestation model derived from the Sanctum project. We expect devices to have a root key, we do some key derivation based off that during the boot process, then we produce reports (signed by the Security Monitor) showing a measured boot process. Any enclave can then ask for what its initial state measurement and configuration / protections were enabled when the enclave was created. One of these protections it can ask for is "on chip memory protection".

5.6.2. So, assuming your platform has cache configurable such that it can support a scratchpad, we build that scratchpad memory, load the enclave into that memory (rather than main memory) and execute it from there. This is transparent to the enclave until it runs out of space (which is fast, so run small things in there). Larger code bases would require a paging system. We have a full software implementation of an integrity protected and encrypted memory paging system (quite slow as it is software), however this shows an example of how one might implement on enclave page cache plus enclave page memory.

5.7. Security – Bug Disclosure

5.7.1. Because there are no products using Keystone, we do not have a security bug disclosure process, however we hope to move in this direction as Keystone gains product adoption.

6. Proposal: The TAC recommends to the board adopt Keystone as a CCC process.

6.1. As a reminder, the TAC must approve, legal review must happen, then the board will vote for the final pass of accepting the project.

6.2. All voting members of the TAC on the call have voted **'yes' to accept.** This completes step 1 approval.

6.3. TAC Mentor – If needed, we'd like to have folks that might be willing to act as a mentor.

7. TAC Whitepaper Review

7.1. https://docs.google.com/document/d/17PhrIXvFJsAIJryYjpezmfdSI1BSB1x1tE2FTbriHyc/edit

7.2. Between now and the next meeting please add any comments or suggestions around content / flow / etc.

8. GitHub Pull Request / Issues

8.1. Please review 57 and 58 as those two simply need approval before they are merged.

8.2. There are no new issues, and everything has been reviewed.

9. Summer Schedule

9.1. We will continue to meet both days in August.

10. Scoping Follow-up

10.1. The scoping doc is listed on the website, we'd like to link to something that is more of a statement rather than the current document.

10.2. We'd like to change the tense to present tense and update the text to be definitive rather than open items.

11. Avalon

11.1. Avalon is the "blockchain" part of the Trusted Compute Framework (TCF) which recently joined the CCC. Our feedback was for them to pick a different name; however, we are not sure if that has happened yet.

11.2. If anyone has any questions about the transition, or needs a contact inside Hyperledger, please feel free to reach out to Ry Jones

Action Items

1. [Seth] Please bring up the scoping document in the Outreach meeting and discuss ways to make it more relevant as a public document.

2. [David Kohlbrenner] Please provide a list of the licenses used for crypto implementations, specifically to ensure that they are all OSI approved.

3. [Stephano] Send an email out regarding Enarx receiving an email list (groups.io) instance. [**DONE**]

Meeting adjourned at 8:30 am PT on July 23, 2020. The next conference call will be scheduled for Thursday August 6.

DRAFT

Respectfully submitted by Stephano Cetola, Acting Secretary, on July 25, 2020.