Technical Advisory Council (TAC) Meeting

September 21, 2023

CONFIDENTIAL COMPUTING CONSORTIUM

This meeting is being recorded.

The Confidential Computing Consortium

A community focused on open source licensed projects securing DATA IN USE & accelerating the adoption of Confidential Computing through open collaboration

Every member is welcome; every project meeting our criteria is welcome.
We are a transparent, collaborative community.

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

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.

CONFIDENTIAL COMPUTING CONSORTIUM

Agenda

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Congratulations to rust-spdm
4. Tech Talk: Oblivious RAM - Prof. Elaine Shi (30 min)
5. 2023 TAC Goals: Cross project collab survey. (5 min)
6. CISA RFI: working session (30+ min)
7. Action Items: tbd
8. Any other business
    a. Next meeting agenda
        - Budget / 2024 planning
    b. Issues/Pull requests
        - Refine mission statement

Roll Call

Quorum requires **4** or more voting reps:

* *TAC chair*

Member	**Representative / Alternate**	**Email**
Accenture	Giuseppe Giordano	giuseppe.giordano@accenture.com
Arm	Nathaniel McCallum / Michael	nathaniel.mccallum@arm.com
Meta Platforms	Eric Northup / Shankaran	digitaleric@fb.com
Google	Cfir Cohen / Catalin Sandu	cfir@google.com
Huawei	Zhipeng (Howard) Huang	huangzhipeng@huawei.com
Intel	Dan Middleton * / Simon Johnson	dan.middleton@intel.com
Microsoft	Dave Thaler / Alec Fernandez	dthaler@microsoft.com
Red Hat	Lily Sturmann / Yash Mankad	lsturman@redhat.com

CONFIDENTIAL COMPUTING CONSORTIUM

Welcome New Community Members

New to the community?

Haven’t introduced yourself at least twice?

Let us know

- your name
- where you are joining from
- your main Confidential Computing interest

CONFIDENTIAL COMPUTING CONSORTIUM

Approval of TAC Minutes

https://github.com/confidential-computing/governance/pull/186

Proposed:
That the minutes of the September 7, 2023 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.

CONFIDENTIAL COMPUTING CONSORTIUM

Tech Talk : Oblivious RAM

Abstract: I will give a brief tutorial of Oblivious RAM (ORAM). Then I will talk about how ORAM evolved from a theoretical concept to large-scale real-world deployment, and the various emerging demands and uses cases of ORAM in both the blockchain community and for traditional cloud services. In particular, I will talk about Signal's deployment of Path ORAM over their billion-sized database, and how ORAM allowed them to cut their 500 servers downto 6 servers.

Finally, I will describe a new initiative to build an open-source Oblivious STL library, aiming to provide an oblivious counterpart of the standard STL library. I will describe our initial efforts at building Oblivious STL. Specifically, I will focus on how using external-memory algorithms techniques can allow us to achieve orders-of-magnitude performance improvement over state-of-the-art implementations for hardware enclaves. In particular, while the literature on ORAM typically uses computational overhead as the performance metric, for hardware enclaves, the number of page swaps is often the dominant metric. Through the help of external-memory algorithms, we can achieve an asymptotical improvement in the number of page swaps.

Bio: Elaine Shi is an Associate Professor at Carnegie Mellon University. Prior to joining CMU, she taught at Cornell and the University of Maryland. Her research interests include cryptography, security, algorithms, mechanism design, and foundations of blockchains. She has won numerous awards such as the Sloan Fellowship, the Packard Fellowship, the ONR YIP award, the NSA Best Science of Cybersecurity Paper award, Cylab Distinguished Alumni Award, and various other best paper awards. Her work on Oblivious RAM and privacy-preserving algorithms have been deployed at a large scale by companies like Signal, Google, and JP Morgan.

2023 TAC Goals

Working copy: https://docs.google.com/document/d/1BLsI0hv9ybHl-FBNqHp6bJzy6ng8yKs__556bTqBswc

“We have increased the impact of the CCC in the ecosystem such that…”

1. **we increased Cross-project Integration [Lily, EricV]**
2. **the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]**
3. **other organizations reference Confidential Computing [MarkN, Howard, Thomas]**
4. **broadened community understanding and awareness of CC [Giuseppe, Cfir, EricN]**
5. **enhanced community D&I [Dan, Nick]**

Project Progression

~~Final call on https://github.com/confidential-computing/governance/pull/90~~

Badge in Annual Review
~~https://github.com/confidential-computing/governance/pull/176~~

Graduation Stage - Dave
https://github.com/confidential-computing/governance/pull/170
https://github.com/confidential-computing/governance/pull/171

Sandbox Stage - Howard
https://github.com/confidential-computing/governance/pull/160

CONFIDENTIAL COMPUTING CONSORTIUM

Progression discussion

- https://github.com/confidential-computing/governance/pull/160
- What additional services do projects want?
  - Gramine: Website
  - Note that existing list came from project requests and voted in by TAC after original policy was created
  - Mentors check in with projects on wishlists (see slide 28)
- Are different tiers / progression levels helpful or necessary?
  - History:
    - initial stage: is it defined enough to accept to the CCC
    - next stage: under development vs in production
  - How to apply criteria to projects with subprojects at different stages?

2023 TAC Goals

Working copy: https://docs.google.com/document/d/1BLsI0hv9ybHl-FBNqHp6bJzy6ng8yKs__556bTqBswc

“We have increased the impact of the CCC in the ecosystem such that…”

1. **we increased Cross-project Integration [Lily, EricV]**
2. **the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]**
3. **other organizations reference Confidential Computing [MarkN, Howard, Thomas]**
    a. **NIST?**
4. **broadened community understanding and awareness of CC [Giuseppe, Cfir, EricN]**
    a. **?**
5. **enhanced community D&I [Dan, Nick]**

CONFIDENTIAL COMPUTING CONSORTIUM

Community Ed Goals

Starter text… “We have increased the impact of the CCC in the ecosystem such that…”

“~~… the ecosystem is more aware of Confidential Computing~~”
“… the ecosystem is more aware of the benefits of Confidential Computing”

As measured by:

- We promoted security research papers on each of the technologies in production in 2023.
    a. As worded this is effort not impact.
    b. consider “H” Factor / Index (impact of citations)
        i. create an author page https://paperpile.com/g/h-index-google-scholar/
- We drafted a survey paper highlighting common strengths and weaknesses across technologies.
- We presented at n conferences…

Attestation Wikipedia Article

Where do we want to do this?

- TAC
- AAA SIG ←
  - Work offline, mail list, updates in the SIG, etc.
- …

Are there other groups we should involve?

- TCG (Henk volunteered)
- …

Any other business / Schedule

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk / Proposal / etc
23 Mar 2023	OE SDK - Radhika		SGX Assurance Tool - Alex Berenzon
6 April 2023	GRC - Mark Novak [3]	[2] Progression - Howard	CDCC - XiaoFeng Wang
20 April 2023		[1] Cross Project - Lily / EricV	
4 May 2023		[4] Education - Cfir et al	VirTEE - Sergio Lopez Pascual (@slp)
18 May 2023	Attestation SIG	[5] D&I - Dan & Nick	Keylime - Thore / Marcio
1 June 2023		[2] Progression pt.2 - Dave/Howard	Bao Project - Sandro / Howard
15 June 2023	Veraison - Thomas Fossati	[2] Progression pt.2 - Dave/Howard	
29 June 2023	CCS	CCS	CCS
13 July 2023		1, 3, or 4	~~Fan Zhang - CDCC second talk~~
27 July 2023	Canceled	n/a	~~SPDM - Jiewen Yao~~
10 Aug 2023	GRC Sig quarterly update	n/a	CHAOSS and D&I - Georg Link SPDM - Jiewen Yao
24 Aug 2023	Outreach update	All / Quarterly Checkup	CISA RFI

1. **we increased Cross-project Integration [Lily, EricV]**
2. **the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]**
3. **other organizations reference Confidential Computing [MarkN, Howard, Thomas]**
4. **grew outbound education [Giuseppe, Cfir, EricN]**
5. **matured community D&I [Dan, Nick]**

CONFIDENTIAL COMPUTING CONSORTIUM

Any other business / Schedule (Continued)

Date	CCC Project Review	TAC Goal Topic	TAC Tech Talk
07 Sept 2023			MPC/FL + TEE and FHE - Kevin (Inpher)
21 Sept 2023			Oblivious RAM: from theory to large-scale real-world deployment - Elaine Shi (Carnegie Mellon University)
05 Oct 2023			
19 Oct 2023			
02 Nov 2023			
16 Nov 2023			
30 Nov 2023			
14 Dec 2023			
14 Dec 2023	Cancel?		

1. **we increased Cross-project Integration [Lily, EricV]**
2. **the CCC hosts s/w projects adopted by the ecosystem [Dave, Howard, Dan]**
3. **other organizations reference Confidential Computing [MarkN, Howard, Thomas]**
4. **grew outbound education [Giuseppe, Cfir, EricN]**
5. **matured community D&I [Dan, Nick]**

CONFIDENTIAL COMPUTING CONSORTIUM

Next Agenda (2023-10-05)

1. Welcome, roll call, introduce any first-time attendees
2. Approval of minutes
3. Action item review
4.
5. 2023 Goals
    a. Progression:
    b. TAC Goals:
6. Annual Report/Update:
7. Tech Talk:
8. Any other business
    a.
    b.

CONFIDENTIAL COMPUTING CONSORTIUM

Action Item Review

1. [Dan/Kurt] 2/9: to look into a communication channel (mail list?) for discussing cross-project security concerns
    a. 3/21: Mail list created, need mentors to contact their projects for the right person to monitor
    b. 4/20: ~~[Thomas] Veracruz~~ (contacted: Derek or Mathias); OE (Radhika)
    c. 5/4: Remaining mentors/projects; Kurt will ping the TAC list again.
2. [Kurt] 3/23: revise the Project review timeline and Tech Talk slides to show current status (In progress)
3. [Kurt] ask Outreach committee if they needed a source .md file for the “Confidential Computing: Hardware-Based Trusted Execution for Applications and Data” white paper
4. [Kurt] get the latest recommendations on how the LF LFX license scans are started and what code-bases are supported (In progress, Kurt to get LFX Security to come to a future TAC)
5. [Pawan] find a TCG expert for review the GRC Customer Guide wording, maybe Henk Birkholz or Ned Smith
6. [Kurt] work with Tyler on the next steps to take the proposal to the Governing Board for approval (In progress)
7. [Dave] update the Project Progression PRs and create a new PR for the name changes
8. [Kurt] cleanup charters after DM merges #90 ("Projects" directory for the charters not the current "project-charters" directory in governance)
9. [Kurt] sync with Lily for kicking off a cross-project maintainer's meeting (discussed at CC Summit)
10. Dave volunteered to create an author listing for Google Scholar
11. Kurt to see if LF expense template can be shared and linked to this document

Time permitting: Review of open issues and PRs

Current open issues in the Governance repo:
https://github.com/confidential-computing/governance/issues

Current open PRs in the Governance repo:
https://github.com/confidential-computing/governance/pulls

CONFIDENTIAL COMPUTING CONSORTIUM

Project	Proposed by	TAC Approved	Tech. Charter	IP Assigned	Board Presentation	Board Approved	Annual Review	Mentor	Webinar
Enarx	Red Hat	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	10 MAR 2022	Nick Vidal	JAN 2021
OE SDK	Microsoft	31 OCT 2019	Yes	Yes	31 OCT 2019	Yes	24 FEB 2022	Dave Thaler	MAR 2021
Gramine	UNC Chapel Hill	2 APR 2020	Yes	Yes	1 DEC 2021	15 SEP 2021	4 NOV 2021	Eric V	FEB 2022
Keystone	UC Berkeley	23 JUL 2020	Yes	Yes	24 JUN 2021	MAR 2021	13 JAN 2022	Lily	JUN 2021
Occlum	Ant Financial	20 AUG 2020	Yes	Yes	10 SEP 2020	15 SEP 2021	17 NOV 2022	Tate Tian	MAY 2021
Veracruz	Arm	3 SEP 2020	Yes	Yes	19 NOV 2020	14 APR 2021	12 JAN 2023	Thomas F	APR 2021
Veraison	Arm	4 FEB 2022	Yes	Yes	16 MAR 2022	18 May 2022	15 JUN 2023	Howard Huang	NOV 2021

SIG / WG	Proposed by	TAC Approved	Tech. Charter	Board Presentation	Annual Review	Mentor	Webinar
CCC-Attestation SIG	TAC	Yes	Yes	18 MAR 2021	21 APR 2022	Dan	21 JUNE 2022
GRC SIG	TAC	Yes	Yes	21 SEP 2022	Quarterly	Mark Novak	

CONFIDENTIAL COMPUTING CONSORTIUM

Deferred topics / Backup

Project Website Funding

Gramine and Veraison have both asked for website updates

- Rough estimate approximately $5K each ($16k for github page)
- Existing budget allocated $10K total for all projects for “Project IT Services and Collab Tools” which would cover website redesign
- Gramine also needing VPS Cloud services from the same budget item

1) Gramine VPS could be funded out of “Test Infrastructure/Hardware” budget ($10K) and that would allow all the 10K from Project IT Services to be used on websites
2) The TAC could get Governing Board approval for additional funding for Project IT Services
3) The TAC could also/instead get approval to allow funding to be shifted from Test to IT
4) Seek competitive bid from outside LF?
5) Associate this spend level with progression level

CONFIDENTIAL COMPUTING CONSORTIUM

TAC Budget (From approved budget 2/28/23 Final)

Description	2022 Approved Budget	2023 Approved Budget	Notes	Area
License Scanning	$12,000	$0	LF Security	Project support
Test infrastructure (capital or non-capital)	$75,000	$60,000	$10k/project x 6 projects	Project support
IT Services and Collab Tools	$3,864	$15,000	website, slack, groups,io	Project support Community development & DCI
Consortium IT Services and Collab Tools	$100,000	$10,000	Misc. budget for use by projects	Project support
Staff Travel	$0	$60,000	$10k/project x 6 projects	Project support (combined with other travel)
Hosting and other costs	$10,000	$0	Software	Project support
Outreachy (internships/community support)	$52,000	$32,000	Outreachy ($8k x 4 projects)	Community development & DCI Project support
Community Support		$100,000	Part-time Technical Architect	Community development & DCI Project support
Subtotal	$257,781	$277,000		

Reference: CCC project benefits

CCC projects have access to a number of benefits:

- Up to $10K in budget for hardware and software per year
- Funding for one Outreachy intern
- TAC mentor assigned to the project
- Collaboration tools (contact operations@confidentialcomputing.io):
  - Zoom
  - Domain registration and renewals
  - Mailing lists
  - YouTube playlists
  - Slack
- Optional security scanning
- LFX tools (https://lfx.linuxfoundation.org)

CONFIDENTIAL COMPUTING CONSORTIUM

Reference: past TAC tech talk topics

- 2021-10-07: Kata containers
- 2021-10-21: Protecting critical infrastructure
- 2021-12-02: RISC-V security overview
- 2022-01-13: Homomorphic Encryption
- 2022-01-27: OP-TEE and Trusted Services
- 2022-02-10: Confidential computing LFX mentorship
- 2022-03-10: Overview of TCG confidential computing
- 2022-04-07: Governance
- 2022-04-21: Code Scanning via LFX Security
- 2022-05-05: IETF Trusted Execution Environment Provisioning (TEEP)
- 2022-05-19: Logging and error reporting in confidential computing
- 2022-06-02: Multi-TEE systems: PCI-SIG WG
- 2022-06-30: Blueprints for Enclaves
- 2022-09-22:
- 2022-10-06: HC / RISC-V Security
- 2022-12-01: Best Practices for Creating an Inclusive Community
- 2023-02-25: RISC-V AP-TEE
- 2023-03-09: eBPF
- 2023-03-23: SGX Assurance Tool

Annual reports

governance/project-progression-policy.md at main · confidential-computing/governance (github.com)

“The review includes the following:

1. Review whether any answers to the project's submission template or Technical Charter have changed, and if so, review the new answers. A representative from the project is responsible for presenting any deltas to the template answers since the last review, if any. If there are no changes, there is nothing to review here.
2. Review the project's progression status to determine whether the project is in the stage that accurately reflects its needs and goals. For example, is it already ready to move to another progression level? Is it on track at the current level? Is any action needed from the TAC (e.g., change in or addition to any project mentor(s))? If nothing has changed significantly, there may be nothing to review here.
3. Review any budget allocations relevant to the project, and whether any adjustments are needed.
4. Review license scans provided by the Linux Foundation. Provide feedback on any outstanding issues and evaluate the scanning service from the project's perspective.

Projects are encouraged to proactively inform the TAC when something changes that affects their submission template or Technical Charter (changing a License, security reporting process, CoC, etc.), rather than waiting for the next annual review.”

Reference: CCC project expectations

CCC projects are expected to:

- Participate actively in CCC activities (webinars, newsletters, events, etc.)
- Notify the TAC and Outreach committees of relevant news
- Participate in an annual review with the TAC
- Inform the TAC when dependencies change so records can be updated
- Maintainers should take the Linux Foundation's free Inclusive Open Source Community Orientation training course
- Transfer trademarks and domain registrations to the Linux Foundation

CONFIDENTIAL COMPUTING CONSORTIUM