The Road Ahead: How Confidential Computing Will Evolve in the 2020s and Beyond

Sal Kimmich, Tech Community Architect
13 March 2024

Confidential Computing Consortium

Confidential Computing Consortium


cisco

CRYPTOSAT
TRUST IN SPACE

CYSEC

EDGELESS
SYSTEMS

AMD

AMPERE

anjuna

蚂蚁集团
ANT GROUP

MARVELL

NVIDIA

Opaque

Rivos

FUJITSU

GENXT

hushmesh

iExec

BeeKeeperAI™

ByteDance

CanaryBit

CANONICAL

SAMSUNG

spectro cloud

SUSE

ULTRAVIOLET

vmware

Linaro

MIT Connection Science

OASIS FOUNDATION

RISC-V®

ACURAST

CHMRC
LOCAL IMPACT | GLOBAL COLLABORATION

Distributed Ledger Technology
Research Foundation

Fraunhofer
SIT

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

CONFIDENTIAL COMPUTING
CONSORTIUM

Confidential Computing Consortium

- Confidential Computing Definition:
  - The protection of **data in use** by performing computation in a **hardware-based, attested** Trusted Execution Environment.

- Today We Will Cover
  - The State of Confidential Computing - and at OC3!
  - Key Challenges We're Overcoming in the Field
  - Ways to Stay at the Forefront of Confidential Computing

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Compute For Financial Services

- **Securing A Year's Worth of Transactions**
  - Microsoft's Experience with 25 billion in annual credit card Transactions
  - Azure Key Vault Managed HSM and Confidential Computing for secure financial data processing, illustrating the platforms' readiness for sensitive workloads

This example serves as a blueprint for future migrations of high-stakes data to cloud

Moving Microsoft's $25 billion per year credit card processing system to Azure Confidential Computing

In a world of Confidential Compute for Medicine

- Today, you will learn about how the University Clinic Freiburg moved to cloud with Confidential Kubernetes on AMD SEV-SNP allowed the clinic to achieve a secure, accelerated cloud migration.
- Enabling researchers globally to collaborate on cloud without compromising patient privacy, for the first time

Case study: University Clinic Freiburg moves to the cloud with Confidential Kubernetes

Confidential Computing for Human Rights

- When fighting modern slavery, Intel technology enables the Private Data Exchange to leverage Confidential Computing, which processes sensitive data out of view from unauthorized software or system administrators.
  - Organizations like Hope for Justice and Slave-FreeAlliance have joined the effort to find victims, as well as perpetrators. The Private Data Exchange is a innovative project in partnership with Intel and Edgeless, to develop a platform to protect sensitive information
  - This project will enable multiple global organizations to collaborate and share analyses to prevent human trafficking, and respond to situations of exploitation, and ensure victims receive the support they need while shielding their confidential information or regulated data.

Private Data Exchange – Leveraging Confidential Computing to Combat Human Trafficking and Modern Slavery

Confidential Compute for AI

- With Nvidia's H100 AI accelerator becoming available, Confidential Computing can finally be applied to state-of-the-art AI workloads
  - Running AI workloads still requires meaningful end-to-end attestation and end-to-end encryption. Only with these, Confidential AI can deliver actual value
  - Looking towards the Future: this talk will also focus on AI inference and discuss how the following security goals can be achieved in practice:

Easy: Protection of AI workloads against the infrastructure (for secure cloud migration)

Hard: Protection of user data from AI SaaS providers

Confidential AI inference in practice: What's required and how to implement it

Confidential Compute for AI: SPDM-RS

DMTF's Security Protocol and Data Model (SPDM) Specification

This project provides a Rust language implementation of SPDM, IDE_KM and TDISP. These protocols are used to facilitate direct device assignment for Trusted Execution Environment I/O (TEE-I/O) in Confidential Computing: defining messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media to authentication of components, firmware measurement and protection of data in flight.

In machine learning, for example, these protocols can be used to build a trusted connection between a GPU's TEE and a CVM to accelerate performance

github.com/ccc-spdm-tools/spdm-rs

The Current State of Technology

Addressing Key Challenges:

- **Remote Attestation**: ensuring that a system's hardware and software configurations meet specific security standards before engaging in sensitive computation
- **Standardizing Security with ABIs**: Secure Primitive Application binary Interfaces (ABIs) offer a stable method for building secure applications across diverse computing environments, promoting interoperability and enhancing security
  - Secure By Design: Understanding how secure primitives and ABIs form the backbone of trust and security in TEEs, ensuring data integrity and confidentiality
  - Interoperable for Innovation: Standardized ABIs foster cross platform compatibility and encourage innovation within a Confidential Computing ecosystem

Looking Towards the Road Ahead

Progress: Massive strides have been made in Confidential Computing, as more industries recognize the potential to transform data privacy and security

- Confidential Computing today used in **financial services**, in **medicine**, in the **GPU utilization of sensitive data** and the **prevention of human trafficking**
- The demand is rapidly growing as clear use cases for Confidential Compute are showing what we can build when we **make privacy and security a top priority**

Understanding CCC Special Interest Groups

- **Linux Foundation Special Interest Groups (SIGs)**
- Special Interest Groups (SIGs) within the Linux Foundation are collaborative groups that focus on specific areas of interest in the broader landscape of Open Source projects and technologies. SIGs play a crucial role in fostering innovation, sharing knowledge, and working on common goals within their respective domains. Members of SIGs include industry professionals, developers, researchers, and **anyone passionate** about contributing to the advancement of open-source technologies.

- **SIGs in the Confidential Computing Consortium (CCC)**
- The Confidential Computing Consortium (CCC) supports several SIGs focused on different aspects of Confidential Computing. These groups work on initiatives such as developing open standards, creating reference architectures, and enhancing the security and usability of Confidential Computing technologies.

Understanding CCC Special Interest Groups

Regulators and Lawyers, Auditors and GRC: For updates and developments in CC regulation, we suggest joining the **Governance, Risk and Compliance SIG**

Researchers and Developers: For more information on the cutting edge of development for CCC member technologies, we suggest joining the **Attestation SIG**

confidentialcomputing.io/about/committees/

Anyone passionate can join live to any of our SIG meetings: you can simply join in on the zoom link to get involved. All CCC meetings are recorded and available for review.

For more information on all CCC member technologies in this area, join our mailing list: lists.confidentialcomputing.io/g/main/subgroups

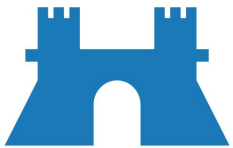
We Welcome Open Source Projects to the CCC

We support Open Source projects in Confidential Computing, and there are many great ways to get involved!

- **OS Project Adoption**: We help you understand, onboard and engage
- **OS Ecosystem Collaborations:** Technical and Educational opportunities

Individual Contributors

- OS Project Contributions
- CCC Mentorship Program







CONFIDENTIAL COMPUTING CONSORTIUM

Challenges we're working on together

- **Technical Complexity and Integration:** Detailing the complexities involved in integrating TEEs with existing infrastructure and the need for technical expertise
- **Interoperability and Standards:** Developing industry-wide standards and regulatory communication to support and adopt different TEE technologies
- **Awareness and Understanding:** Addressing the gap in awareness about the benefits and capabilities of Confidential Computing

Best Ways to Get Involved

Our meetings are open, and also **recorded for anyone to review**

The Attestation SIG meets bi-weekly on Tuesday's at 9:00am Pacific Time.

EMAIL US | MEETINGS | MEETING RECORDINGS | MAILING LIST | MEETING LINK | SLACK

TAC Subcommittee: Governance Risk & Compliance Special Interest Group (GRC-SIG)

The GRC SIG focuses on:

1) connecting confidential computing development community – CSPs, hardware vendors, ISVs, and customers – with the creators of regulatory frameworks with the goal of crafting regulations around confidential computing that result in better security outcomes, and

2) creation of governance patterns that ease development, deployment and operation of confidential computing applications in ways that are compliant and secure. The GRC charter document can be accessed here.

The GRC SIG meets every week on Wednesday's at 7:00am Pacific Time.

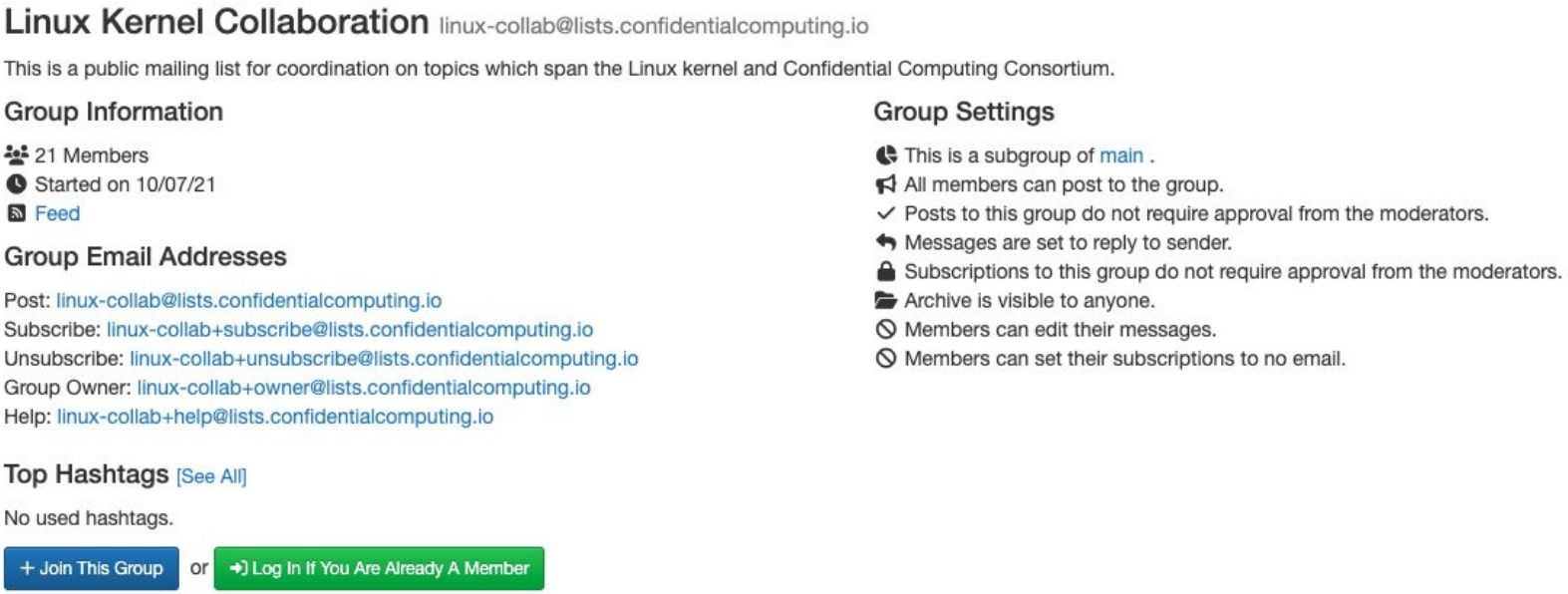
EMAIL US | MEETINGS | MEETING RECORDINGS | MAILING LIST | MEETING LINK | SLACK

TAC Subcommittee: Linux Kernel Special Interest Group (Linux Kernel-SIG)

The Linux Kernel SIG seeks to accelerate Confidential Computing feature velocity in the Linux kernel. By creating a working group in the CCC we foster community dialog to develop common infrastructure and approaches to increase cross architecture reuse and reduce upstream maintenance burden. The group augments but does not replace existing upstream enabling mechanisms. Decisions are still based on consensus and discussed on the Linux kernel development mailing lists.

Best Ways to Get Involved

Our mailing lists are open and cover topics central to Confidential Computing



Linux Kernel Collaboration linux-collab@lists.confidentialcomputing.io

This is a public mailing list for coordination on topics which span the Linux kernel and Confidential Computing Consortium.

Group Information

21 Members
Started on 10/07/21
Feed

Group Email Addresses

Post: linux-collab@lists.confidentialcomputing.io
Subscribe: linux-collab+subscribe@lists.confidentialcomputing.io
Unsubscribe: linux-collab+unsubscribe@lists.confidentialcomputing.io
Group Owner: linux-collab+owner@lists.confidentialcomputing.io
Help: linux-collab+help@lists.confidentialcomputing.io

Group Settings

This is a subgroup of main .
All members can post to the group.
Posts to this group do not require approval from the moderators.
Messages are set to reply to sender.
Subscriptions to this group do not require approval from the moderators.
Archive is visible to anyone.
Members can edit their messages.
Members can set their subscriptions to no email.

Top Hashtags [See All]

No used hashtags.

+ Join This Group or Log In If You Are Already A Member

CONFIDENTIAL COMPUTING CONSORTIUM

Best Ways to Get Involved

Confidential Computing, what would **you** like to share with the world?

We have an entire team dedicated to **CC Technical Demos**

Outreach Committee

The Outreach Committee is responsible for designing, developing, and executing community outreach efforts. The Outreach Committee coordinates with the Governing Board, Technical Advisory Committee, and other community projects to maximize the outreach and visibility of the CCC's effort to drive awareness of Confidential Computing.

The Outreach Committee meets bi-weekly on Wednesday's at 8:00am Pacific Time.

EMAIL US | MEETING RECORDINGS | MAILING LIST | MEETING LINK | SLACK

Challenges we're working on together

- **Technical Complexity and Integration:** Detailing the complexities involved in integrating TEEs with existing infrastructure and the need for technical expertise
- **Interoperability and Standards:** Developing industry-wide standards and regulatory communication to support and adopt different TEE technologies
- **Awareness and Understanding:** Addressing the gap in awareness about the benefits and capabilities of Confidential Computing

confidentialcomputing.slack.com

We Hope You Enjoy OC3!