Confidential Computing devroom - Welcome!

Fabiano Fidêncio, Fritz Alder, Ilaria Battiston, Jo Van Bulck, Steffen Eiden

February 1, 2025

🏠 FOSDEM 2025

whoami

Fabiano Fidêncio

Intel

Fritz Alder

NVIDIA

Ilaria Battiston

CWI Amsterdam

Jo Van Bulck

KU Leuven

Steffen Eiden

IBM

Confidential computing disclaimer

Many definitions of confidential computing may exist.

Today, we take the one from the Linux Foundation's *Confidential Computing Consortium*.

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing is the protection of **data in use** by performing computation in a **hardware-based**, **attested** **Trusted Execution Environment** (TEE).

Definition from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`

Key properties

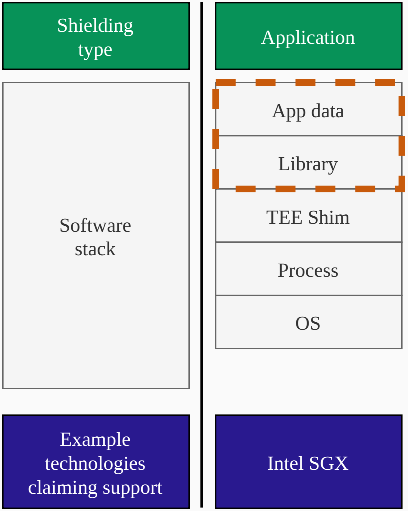
Common properties:

- Data confidentiality
- Data integrity
- Code integrity

Contextual properties:

- Code confidentiality
- Authenticated launch
- Programmability
- Attestability
- Recoverability

Definition from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



Shielding type

Application

Software stack

App data

Library

TEE Shim

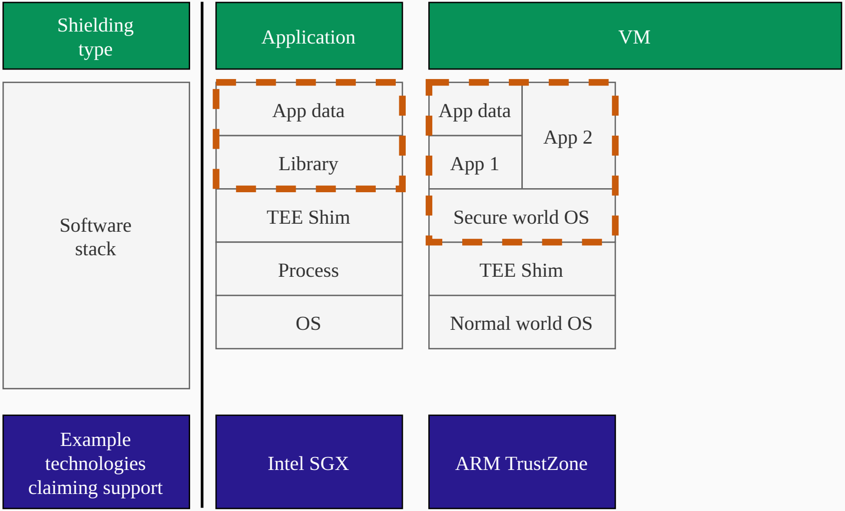
Process

OS

Example technologies claiming support

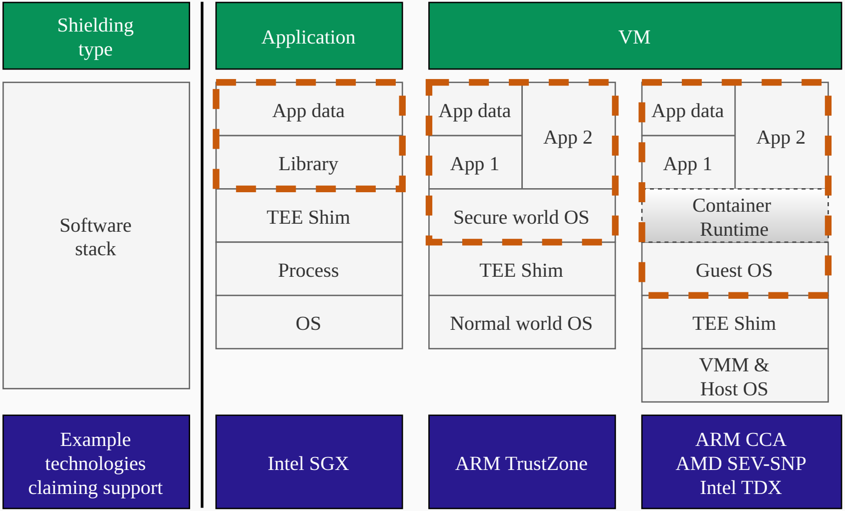
Intel SGX

Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



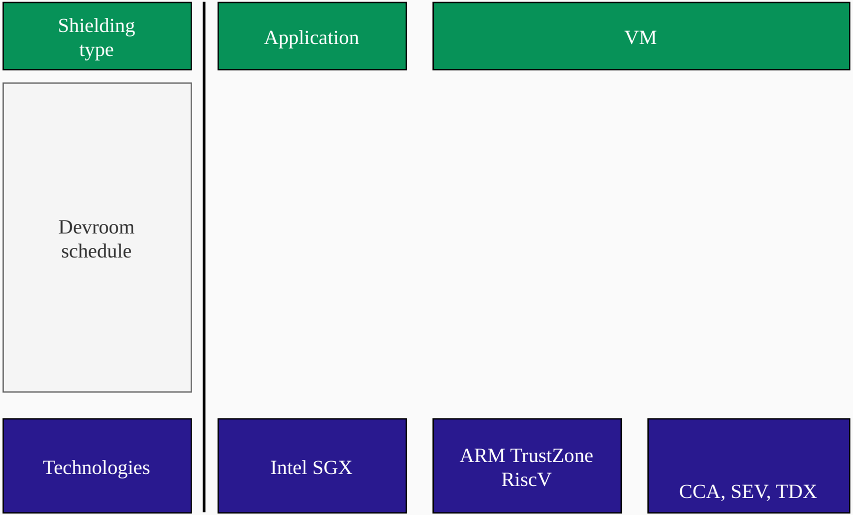
Shielding type	Application	VM
Software stack	App data Library TEE Shim Process OS	App data App 1 App 2 Secure world OS TEE Shim Normal world OS
Example technologies claiming support	Intel SGX	ARM TrustZone

Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



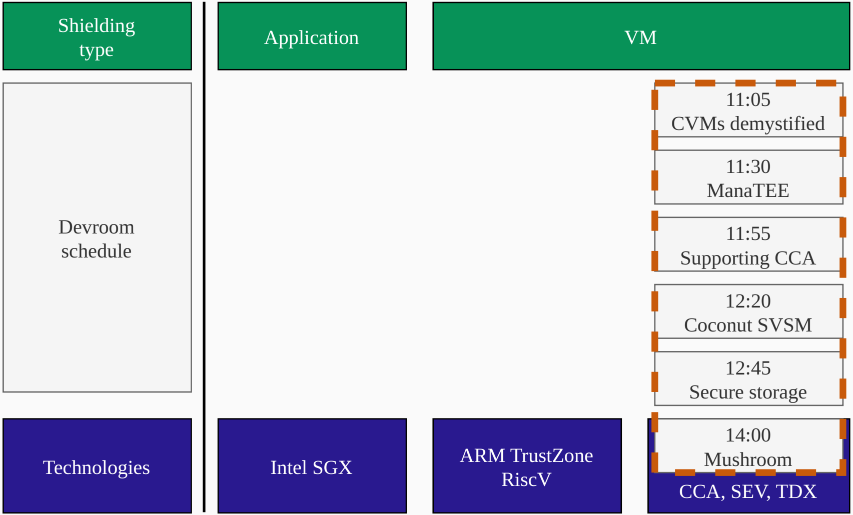
Shielding type	Application	VM	
Software stack	App data Library TEE Shim Process OS	App data App 1 App 2 Secure world OS TEE Shim Normal world OS	App data App 1 App 2 Container Runtime Guest OS TEE Shim VMM & Host OS
Example technologies claiming support	Intel SGX	ARM TrustZone	ARM CCA AMD SEV-SNP Intel TDX

Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



Shielding type	Application	VM	
Devroom schedule			
Technologies	Intel SGX	ARM TrustZone RiscV	CCA, SEV, TDX

Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



Shielding type

Application

VM

Devroom schedule

11:05 CVMs demystified

11:30 ManaTEE

11:55 Supporting CCA

12:20 Coconut SVSM

12:45 Secure storage

14:00 Mushroom

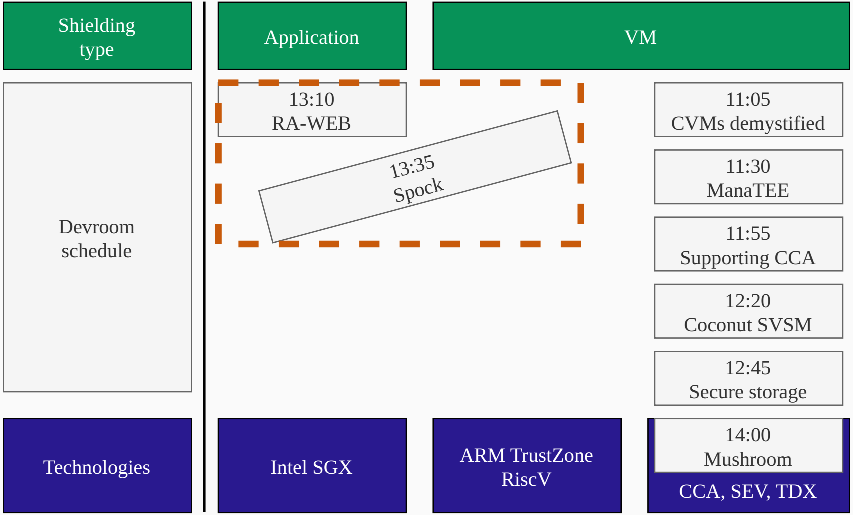
Technologies

Intel SGX

ARM TrustZone RiscV

CCA, SEV, TDX

Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



Shielding type

Application

VM

Devroom schedule

13:10 RA-WEB

13:35 Spock

11:05 CVMs demystified

11:30 ManaTEE

11:55 Supporting CCA

12:20 Coconut SVSM

12:45 Secure storage

14:00 Mushroom

Technologies

Intel SGX

ARM TrustZone RiscV

CCA, SEV, TDX

Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`

Where are we going?

2024	2025
25 submissions, **8 accepted**	**15 submissions**, **9 accepted**

Where are we going?

2024	2025
25 submissions, **8 accepted**	**15 submissions**, **9 accepted**
	Attestation devroom:
	23 submissions, **8 accepted**

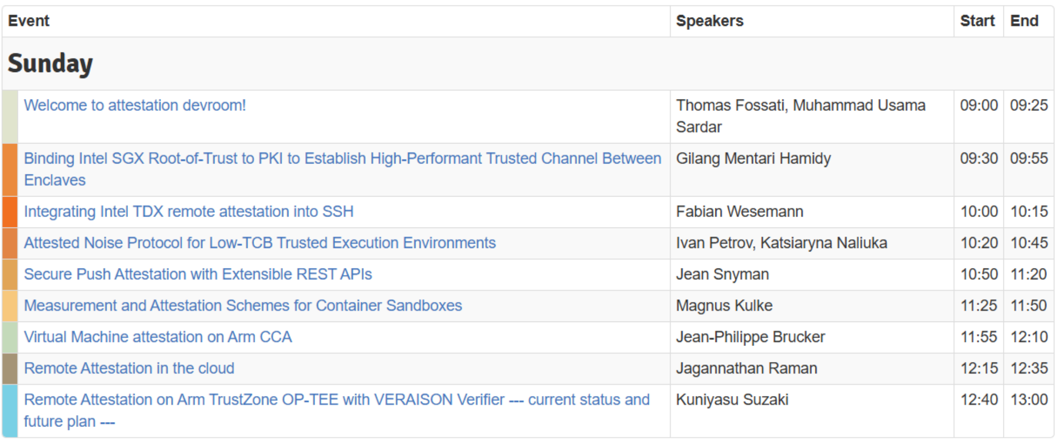
Where are we going?

2024	2025
25 submissions, **8 accepted**	**15 submissions**, **9 accepted** Attestation devroom: **23 submissions**, **8 accepted** And at least 2 other CC-related talks

19 talks related to confidential computing @ FOSDEM 2025!

40 submissions!

Attestation devroom on Sunday! Room K.4.401



Event	Speakers	Start	End
Sunday			
Welcome to attestation devroom!	Thomas Fossati, Muhammad Usama Sardar	09:00	09:25
Binding Intel SGX Root-of-Trust to PKI to Establish High-Performant Trusted Channel Between Enclaves	Gilang Mentari Hamidy	09:30	09:55
Integrating Intel TDX remote attestation into SSH	Fabian Wesemann	10:00	10:15
Attested Noise Protocol for Low-TCB Trusted Execution Environments	Ivan Petrov, Katsiaryna Naliuka	10:20	10:45
Secure Push Attestation with Extensible REST APIs	Jean Snyman	10:50	11:20
Measurement and Attestation Schemes for Container Sandboxes	Magnus Kulke	11:25	11:50
Virtual Machine attestation on Arm CCA	Jean-Philippe Brucker	11:55	12:10
Remote Attestation in the cloud	Jagannathan Raman	12:15	12:35
Remote Attestation on Arm TrustZone OP-TEE with VERAISON Verifier --- current status and future plan ---	Kuniyasu Suzaki	12:40	13:00

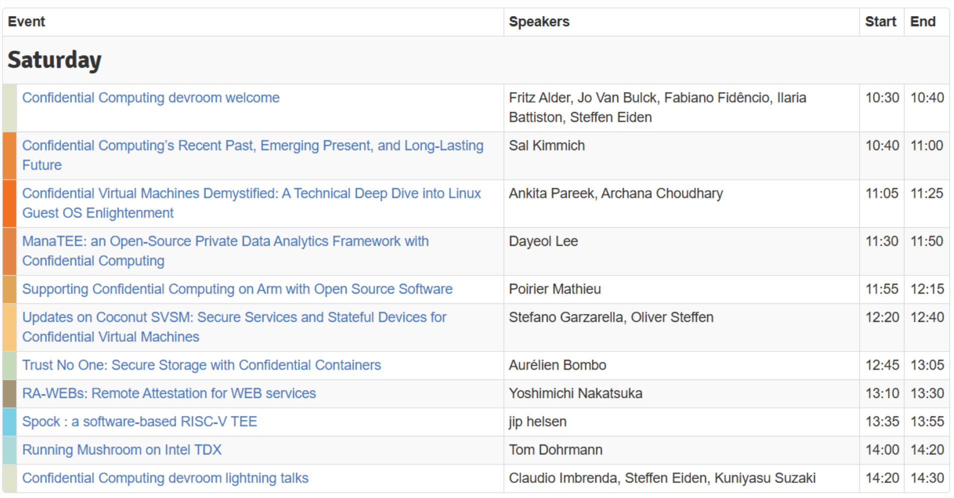
`https://fosdem.org/2025/schedule/track/attestation/`

Honorable mentions

- “Enabling AMD SEV technology in Xen Hypervisor.” – Andrei Semenov
  Virtualization and Cloud Infrastructure devroom [Sunday, 4pm UB4.132]
- “Latest implementation of AMD SEV-SNP in OVMF” – Richard Lyu
  Open Source Firmware, BMC and Bootloader decroom [Saturday, 12:40 UB4.136]
- . . . ?

Thank you to all submissions we could not fit! *Retrievable Secrets for Confidential Guests on s390* (Claudio Imbrenda), *A Game of TEEs: How CC keeps diverging itself from simplicity and wide adoption* (Klaus Heinrich Kiwi), *A persistent vTPM through remote storage* (Sören Langenberg) *Why do current remote attestation methods not suit VM-type CC?* (Kuniyasu Suzaki) *CoMPai: Confidential Multi-Party AI* (Krzystztof Baran) *Introducing FUKI, guest firmware in a UKI* (Ani Sinha)

Schedule



Event	Speakers	Start	End
Saturday			
Confidential Computing devroom welcome	Fritz Alder, Jo Van Bulck, Fabiano Fidêncio, Ilaria Battiston, Steffen Eiden	10:30	10:40
Confidential Computing's Recent Past, Emerging Present, and Long-Lasting Future	Sal Kimmich	10:40	11:00
Confidential Virtual Machines Demystified: A Technical Deep Dive into Linux Guest OS Enlightenment	Ankita Pareek, Archana Choudhary	11:05	11:25
ManaTEE: an Open-Source Private Data Analytics Framework with Confidential Computing	Dayeol Lee	11:30	11:50
Supporting Confidential Computing on Arm with Open Source Software	Poirier Mathieu	11:55	12:15
Updates on Coconut SVSM: Secure Services and Stateful Devices for Confidential Virtual Machines	Stefano Garzarella, Oliver Steffen	12:20	12:40
Trust No One: Secure Storage with Confidential Containers	Aurélien Bombo	12:45	13:05
RA-WEBs: Remote Attestation for WEB services	Yoshimichi Nakatsuka	13:10	13:30
Spock : a software-based RISC-V TEE	jip helsen	13:35	13:55
Running Mushroom on Intel TDX	Tom Dohrmann	14:00	14:20
Confidential Computing devroom lightning talks	Claudio Imbrenda, Steffen Eiden, Kuniyasu Suzaki	14:20	14:30

https://fosdem.org/2025/schedule/track/confidential/