Confidential Computing devroom - Welcome!

Fritz Alder, Jo Van Bulck, Fabiano Fidêncio

February 4, 2024

FOSDEM 2024

whoami

Fritz Alder
NVIDIA

Jo Van Bulck
KU Leuven

Fabiano Fidêncio
Intel

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 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

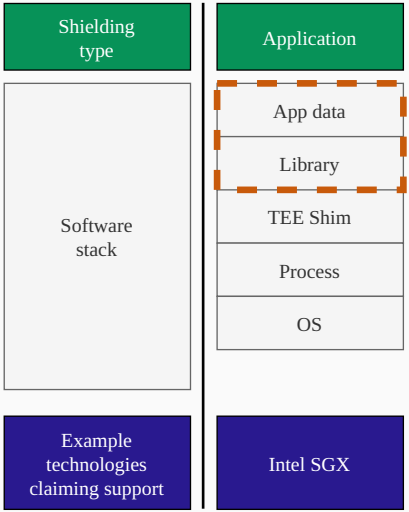
Common properties:

- Data confidentiality
- Data integrity
- Code integrity

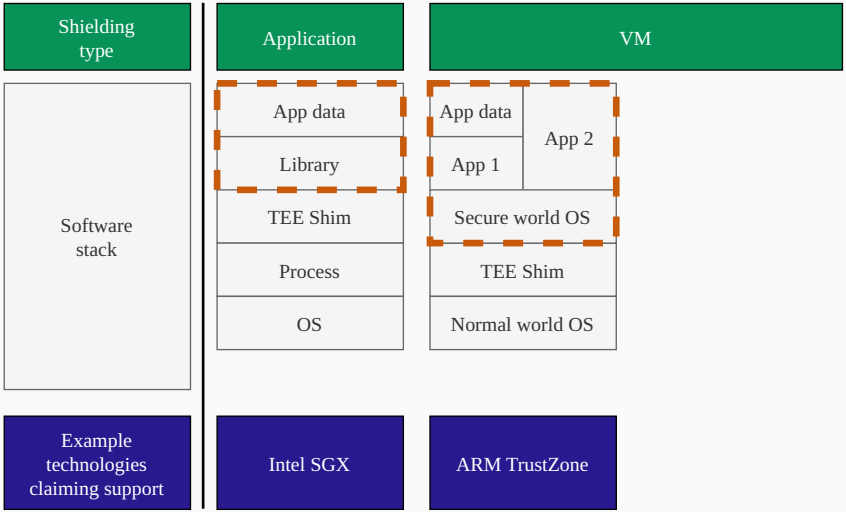
Contextual properties:

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

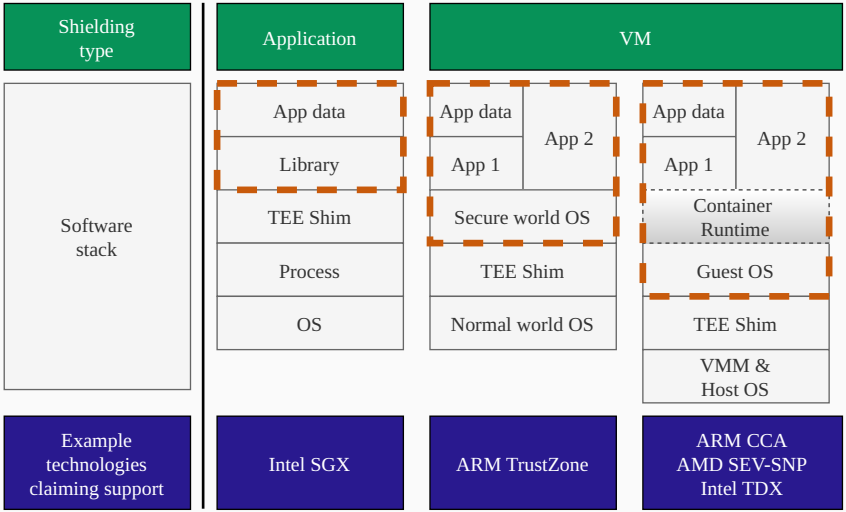
Definition from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



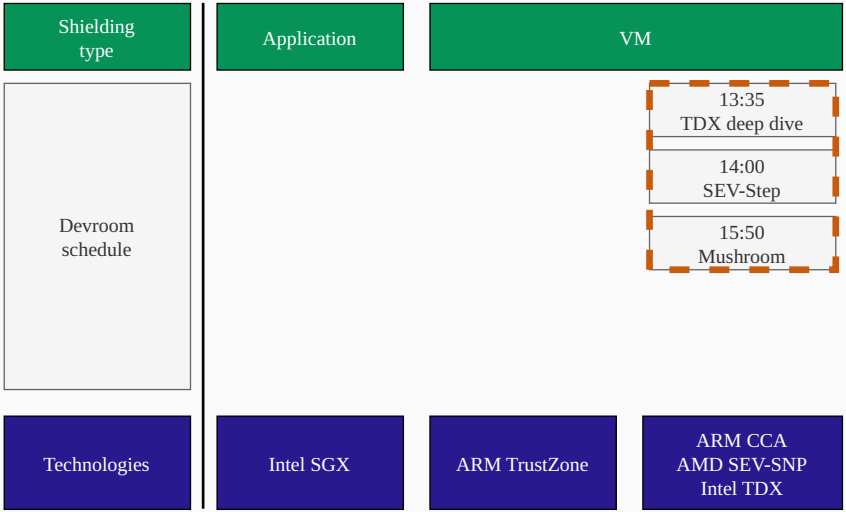
Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



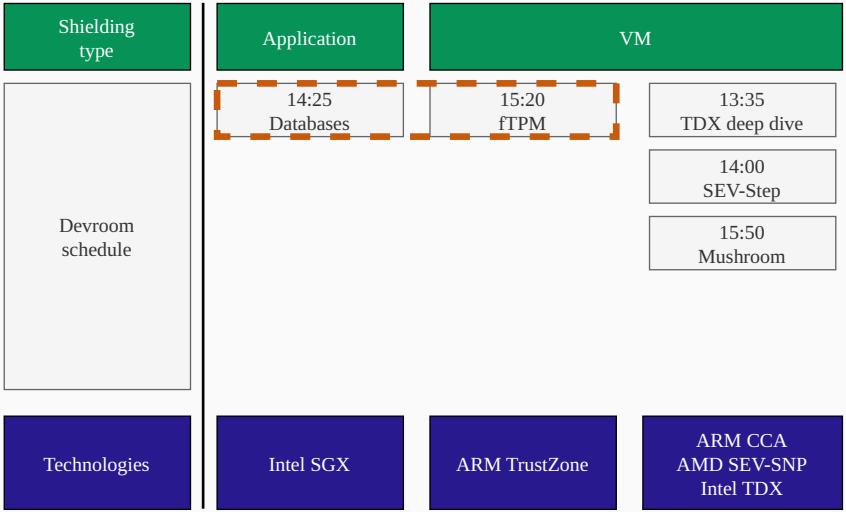
Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



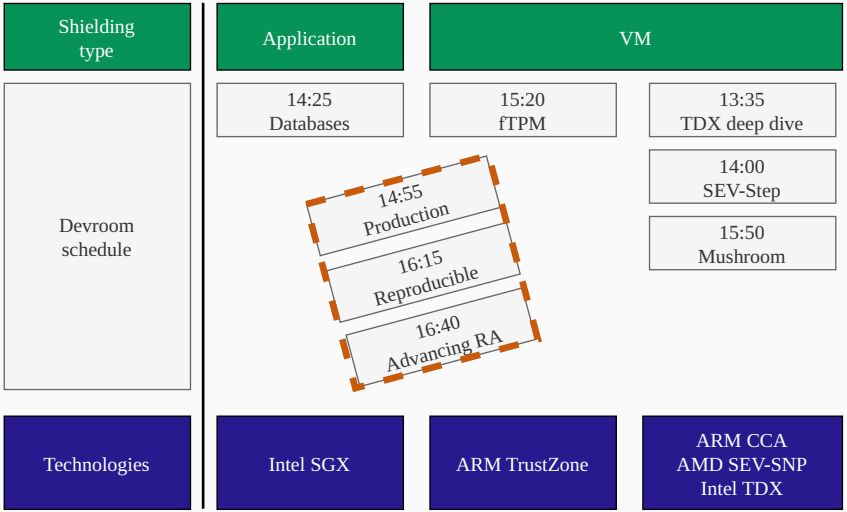
Modified from: *A Technical Analysis of Confidential Computing*, v1.3 (November 2022), `https://confidentialcomputing.io/`



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



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



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

Honorable mentions

- **Project VERAISON** (https://github.com/veraison)
  Also check out Thomas Fossati's talk from FOSDEM'23 in the archives!
- **Confidential Containers** (https://github.com/confidential-containers)
- **Confidential Clusters** (https://github.com/openshift/)
- **CC on OpenStack** (https://www.openstack.org/)
- **RA in Telecom** (https://github.com/nokia/AttestationEngine)
- **Formalizing RA** (https://github.com/CCC-Attestation/formal-spec-TEE/)
- **Pandora** (https://github.com/pandora-tee)
- **Bare-SGX** (https://github.com/jovanbulck/bare-sgx)
- ...

Schedule

Event	Speakers	Start	End
Sunday			
Confidential Computing devroom welcome	Fritz Alder, Jo Van Bulck, Fabiano Fidêncio	13:15	13:30
Intel TDX Deep Dive	Benny Fuhry	13:35	13:55
SEV-Step: A Single-Stepping Framework for AMD-SEV	Luca Wilke	14:00	14:20
Shielding Data, Embracing Openness, Optimizing Performance: A Journey Through Trustworthy Environments for Database Systems	Ilaria Battiston, Lotte Felius	14:25	14:45
The ups and downs of running enclaves in production	Cian Butler	14:55	15:15
Securing Embedded Systems with fTPM implemented as Trusted Application in TEE	Tymoteusz Burak	15:20	15:40
Integrity Protect Workloads with Mushroom	Tom Dohrmann	15:50	16:10
Reproducible builds for confidential computing: Why remote attestation is worthless without it	Malte Poll, Paul Meyer	16:15	16:35
Increasing Trust and Preserving Privacy: Advancing Remote Attestation	Ionut Mihalcea, Thomas Fossati	16:40	17:00

https://fosdem.org/2024/schedule/track/confidential-computing/