Confidential Computing devroom - Welcome!

Fritz Alder, Jo Van Bulck, Fabiano Fidêncio
February 4, 2024

FOSDEM 2024
Fritz Alder
NVIDIA

Jo Van Bulck
KU Leuven

Fabiano Fidêncio
Intel
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).

Key properties

Common properties:
- Data confidentiality
- Data integrity
- Code integrity

Contextual properties:
- Code confidentiality
- Authenticated launch
- Programmability
- Attestability
- Recoverability

Shielding type

Software stack

Example technologies claiming support

Application

App data

Library

TEE Shim

Process

OS

Intel SGX

Shielding type

Application

VM

13:35
TDX deep dive

14:00
SEV-Step

15:50
Mushroom

Technologies

Intel SGX

ARM TrustZone

ARM CCA
AMD SEV-SNP
Intel TDX

Devroom schedule

Honorable mentions

- **Project VERAISON** ([https://github.com/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](https://github.com/confidential-containers))

- **Confidential Clusters** ([https://github.com/openshift/](https://github.com/openshift/))

- **CC on OpenStack** ([https://www.openstack.org/](https://www.openstack.org/))

- **RA in Telecom** ([https://github.com/nokia/AttestationEngine](https://github.com/nokia/AttestationEngine))

- **Formalizing RA** ([https://github.com/CCC-Attestation/formal-spec-TEE/](https://github.com/CCC-Attestation/formal-spec-TEE/))

- **Pandora** ([https://github.com/pandora-tee](https://github.com/pandora-tee))

- **Bare-SGX** ([https://github.com/jovanbulck/bare-sgx](https://github.com/jovanbulck/bare-sgx))

- ...
## Schedule

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

[https://fosdem.org/2024/schedule/track/confidential-computing/](https://fosdem.org/2024/schedule/track/confidential-computing/)