Contribution ID: **10** Type: **not specified**

Confidential Computing MC

CFP closes on July 15th.
Confidential Computing microconferences in the past years brought together developers working secure execution features in hypervisors, firmware, Linux Kernel, over low-level user space up to container runtimes. A broad range of topics were discussed ranging from entablement for hardware features up to generic attestation workflows.

In the past year - guest memfd has been merged, TDX and SNP host support is getting closer to being merged. Next to go in will be support for ARM CCA and RISC V CoVE. In the meantime, there is progress being made on the Trusted I/O front.

But there is still some way to go and problems to be solved before a secure Confidential Computing stack with open source software and Linux as the hypervisor becomes a reality. The most pressing problems right now are:

- Support TEE privilege separation extensions (TDX partitioning and AMD SEV-SNP VM Privilege Levels) both on the guest and host side
- Secure IRQ delivery
- Secure VM Service Module (SVSM) support for multiple TEE architectures
- Trusted I/O software architecture
- Live migration of confidential virtual machines

Other potential problems to discuss are:

- Remote attestation architectures
- Deployment of Confidential VMs
- Linux as a CVM operating system across hypervisors
- Unification of various confidential computing API

The Confidential Computing Microconference wants to bring developers working on confidential computing together again to discuss these and other open problems.

Key attendees:

- Ashish Kalra ashish.kalra@amd.com
- Atish Patra atishp04@gmail.com
- Borislav Petkov bp@alien8.de
- Carlos Bilbao carlos.bilbao@amd.com
- Chao Peng chao.p.peng@linux.intel.com
- Dan Williams dan.j.williams@intel.com
- Daniel P. Berrangé berrange@redhat.com
- Dr. David Alan Gilbert dgilbert@redhat.com
- David Hansen dhansen@linux.intel.com
- David Kaplan David.Kaplan@amd.com

- David Rientjes rientjes@google.com
- Dhaval Giani dhaval.giani@amd.com
- Dionna Amalie Glaze dionnaglaze@google.com
- Elena Reshetova elena.reshetova@intel.com
- James Bottomley jejb@linux.ibm.com
- Jeremy Powell jeremy.powell@amd.com
- Joerg Roedel jroedel@suse.de
- Kirill A. Shutemov kirill.shutemov@linux.intel.com
- Michael Roth michael.roth@amd.com
- Mike Rapoport rppt@kernel.org
- Paolo Bonzini pbonzini@redhat.com
- Peter Gonda pgonda@google.com
- Sean Christopherson seanjc@google.com
- Tom Lendacky thomas.lendacky@amd.com

Primary authors: GIANI, Dhaval; ROEDEL, Joerg (SUSE)

Presenters: GIANI, Dhaval; ROEDEL, Joerg (SUSE)

Track Classification: LPC Microconference Proposals