Contribution ID: **5** Type: **not specified**

Confidential Computing MC

Last years inaugural Confidential Computing microconference brought together plumbers enabling secure execution features in hypervisors, firmware, Linux Kernel, over low-level user space up to container runtimes.

Good progress was made on a couple of topics, most outstanding here is the development of Linux guest support for Intel TDX and AMD SEV-SNP. The patch-sets for both are under intensive review and come close to be merged upstream.

The discussions in the microconference also helped to move other topics forward, such as support for unaccepted memory or deferred memory pinning for confidential guests.

But enabling Confidential Computing in the Linux ecosystem is an ongoing process, and there are still many problems to solve. The most important ones are:

- Design and implementation of Intel TDX and AMD SEV-SNP host support
- Linux kernel memory management changes for secure execution environments
- Support of upcoming secure execution hardware extensions from ARM and RISC-V
- Pre-launch and runtime attestation workflows
- Interrupt security for AMD SEV-SNP
- Debuggability and live migration of encrypted virtual machines
- Proper testing of confidential computing support code

The Confidential Computing Microconference wants to bring together plumbers working on secure execution features to discuss these and other open problems.

Key Attendees:

- Andi Kleen
- Andy Lutomirski
- Borislav Petkov
- Brijesh Singh
- Dr. David Alan Gilbert
- Dave Hansen
- David Hildenbrand
- David Kaplan
- David Rientjes
- Joerg Roedel
- Jun Nakajima
- Kirill A. Shutemov
- Marc Orr
- Mike Rapoport
- Paolo Bonzini

- Peter Gonda
- Sathya Kuppuswamy
- Sean Christopherson
- Tom Lendacky

I agree to abide by the anti-harassment policy

Primary author: ROEDEL, Joerg (SUSE)

Presenter: ROEDEL, Joerg (SUSE)

Track Classification: LPC Microconference Track (CLOSED)