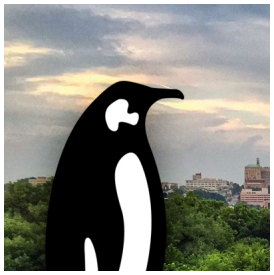

Contribution ID: **22** Type: **not specified**

Confidential Computing Microconference

The 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 was discussed ranging from enablement for hardware features up to generic attestation workflows.

Over the last year there was progress on the development of Confidential Computing in the Linux kernel and user-space. The patch-sets for Intel TDX guest support and AMD SEV-SNP guest support were merged into the Linux kernel. Support for running as a CVM under Hyper-V has also been partially merged.

But there is still some way to go and problems to solve 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 for restricted memory (Unmapped Private Memory patch-set, UPM) is still under development and discussion
- AMD SEV-SNP and Intel TDX host support

Other potential problems to discuss are:

- Support for un-accepted memory
- Confidential Computing support for ARM64
- Attestation workflows
- Secure VM service module (SVSM) and paravisor architecture and implementation (LINUX-SVSM vs. COCONUT-SVSM)
- Confidential Computing threat model
- Secure IO and device attestation
- Intel TDX Connect
- AMD SEV-TIO
- RISC-V CoVE (Task group and patches)
- Debuggability and live migration of confidential virtual machines

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

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

Track Classification: LPC Microconference Proposals