Contribution ID: **9** Type: **not specified**

Confidential Computing Microconference

Encryption technologies which protect data while in transit (SSL, VPNs) and at rest (disk encryption) are available and used for a long time already. Encryption technologies for data while it is processed are a recent addition to CPUs from various vendors. Examples are AMD SEV, Intel TDX and IBM Secure Execution on s390x.

The Linux kernel recently gained support for SEV-ES to protect data in a virtual machine from being accessed by the hypervisor. But this is only the start, Intel TDX is upcoming and AMD SEV will be further enhanced by Secure Nested Paging (SNP). Support for these technologies requires intrusive changes in the Linux kernel to support, for example, memory integrity and secure interrupt delivery to virtual machines.

The Confidential Computing Microconference wants to bring the right people together to propose and discuss solutions to the open problems for supporting these technologies in the Linux kernel and plumbing layer.

Potential open problems to discuss (no particular order):

- Live Migration of Confidential VMs
- Lazy Memory Validation
- APIC emulation/interrupt management
- Debug Support for Confidential VMs
- Required Memory Management changes for memory validation
- Safe Kernel entry for TDX and SEV exceptions
- Requirements for Confidential Containers
- Trusted Device Drivers Framework and driver fuzzing
- Remote Attestation

Supporting links:

- TDX guest support patches
- AMD-SNP guest support and hypervisor support patches. The guest support patches also contain a basic implementation of memory management changes needed for AMD-SNP
- Live Migration using PSP patches
- Alternative method for live migration using a separate vCPU
- Proposed Intel and AMD extensions for safer kernel entry on x86-64
- AMD SEV-SNP Whitepaper describing the page states to keep track of for lazy memory validation and the description of secure interrupt injection using the new #HV vector
- GHCB specification describing the guest-hypervisor protocol for secure interrupt injection
- Discussion about SEV debug support and QEMU patches
- Confidential KATA containers proposal
- SNP guest support driver needed for remote attestation

General Information about Confidential Computing hardware facilities can be found here:

- AMD Secure Encrypted virtualzation
- Intel Trusted Domain Extensions
- ARMv9 Secure Virtualization

Potential attendees (in alphabetical order):

- Andi Kleen ak@linux.intel.com
- Andy Lutomirski luto@kernel.org
- Borislav Petkov bp@alien8.de
- Brijesh Singh brijesh.singh@amd.com

- David Kaplan David.Kaplan@amd.com
- David Rientjes rientjes@google.com
- Joerg Roedel jroedel@suse.de
- Jun Nakajima jun.nakajima@intel.com
- Kirill A. Shutemov kirill.shutemov@linux.intel.com
- Paolo Bonzini pbonzini@redhat.com
- Peter Zijlstra peterz@infradead.org
- Sathya Kuppuswamy sathyanarayanan.kuppuswamy@intel.com
- Sean Christopherson seanjc@google.com
- Tom Lendacky thomas.lendacky@amd.com

I agree to abide by the anti-harassment policy

I agree

Primary author: ROEDEL, Joerg (SUSE)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC