Contribution ID: **120** Type: **not specified**

Fuzzing Device Interfaces of Protected Virtual Machines

Wednesday, 22 September 2021 09:35 (30 minutes)

Both AMD and Intel have presented technologies for confidential computing in cloud environments. The proposed solutions —AMD SEV (-ES, -SNP) and Intel TDX —protect Virtual Machines (VMs) against attacks from higher privileged layers through memory encryption and integrity protection. This model of computation draws a new trust boundary between virtual devices and the VM, which in so far lacks thorough examination.
To enable the scalable analysis of the hardware-OS interface, we present a dynamic analysis tool to detect cases of improper sanitization of input received via the virtual device interface. We detail several optimizations to improve upon existing approaches for the automated analysis of device interfaces. Our approach builds upon the Linux Kernel Library and clang's libfuzzer to fuzz the communication between the driver and the device via MMIO, PIO, and DMA. An evaluation of our approach shows that it performs 570 executions per second on average and improves performance compared to existing approaches by an average factor of 2706.
Using our tool, we analyzed 22 drivers in Linux 5.10.0-rc6, thereby uncovering 50 bugs and initiating multiple patches to the virtual device driver interface of Linux.

I agree to abide by the anti-harassment policy

I agree

Primary authors: HETZELT, Felicitas (TU Berlin); RADEV, Martin; BUHREN, Robert; MORBITZER, Mathias

Presenters: HETZELT, Felicitas (TU Berlin); RADEV, Martin; BUHREN, Robert; MORBITZER, Mathias

Session Classification: Testing and Fuzzing MC

Track Classification: Testing and Fuzzing MC