GI-Herbsttreffen 2009 in Bommerholz

NOVA: Virtualization with a small trusted computing base

Udo Steinberg
udo@hypervisor.org

Technische Universität Dresden
Department of Computer Science
Operating Systems Group

The addition of virtualization support in modern x86 processors has renewed the trend of consolidating multiple guest operating systems on top of a hypervisor in order to improve platform resource utilization and reduce the total cost of ownership. However, if an attacker manages to compromise the hypervisor, the security of all hosted operating systems is at risk.

Therefore, the primary design goal of NOVA was a reduction of the total size of the trusted computing base in order to reduce the attack surface as much as possible. Despite moving most of the virtualization functionality and all device drivers to user mode, our implementation achieves near–native virtualization performance with a TCB that is one to two orders of magnitude smaller than that of existing VMM software.

In this talk I will present the architecture and discuss how the implementation leverages new hardware features, such as multiple cores, CPU and I/O virtualization, and DMA remapping.