BTU Cottbus – Senftenberg
Fakultät 1 / MINT - Mathematik, Informatik,
Physik, Elektro- und Informationstechnik
Institut für Informatik
Lehrstuhl Verteilte Systeme/Betriebssysteme, Prof. Dr.-Ing. Jörg Nolte
Lehrstuhl IT-Sicherheit, Prof. Dr.-Ing. Andriy Panchenko

Brandenburgische
Technische Universität
Cottbus - Senftenberg

INFORMATIK-KOLLOQUIUM

Termin: 28.05.2019, 15.30 Uhr

Ort: BTU Cottbus, ZHG/HS C

Vortragende:

Thomas Prescher, Julian Stecklina (Cyberus Technology GmbH Dresden)

Thema:

LazyFP: Discovering Side-Channels is not a Beach Vacation

Abstract:

In 2018, we jointly discovered and responsibly disclosed the LazyFP microarchitectural side-channel vulnerability (CVE-2018-3665). LazyFP is a Meltdown-type attack on hypervisors and operating systems that use lazy FPU context switching and allows recovery of FPU/SSE/AVX register sets across process and virtual machine boundaries. The underlying microarchitectural flaw is present in all modern Intel Core-based processors.

In this talk, we look at this vulnerability in two ways. On the technical side, we review the different register sets on an x86 CPU and how operating system kernels and hypervisors manage them. We describe how the obscure Lazy FPU context switching optimization together with a microarchitectural weakness form an information disclosure vulnerability. We explain why FPU registers can even contain interesting secrets and how this vulnerability was mitigated.

On the non-technical side, we tell the story of two systems developers working for different companies, one at a small German cyber-security company and one at an American trillion-dollar corporation, finding a security issue in Intel's main product. Looking back on these turbulent events, we detail our personal lessons learned and how we would approach an event like this in the future.

Alle Interessenten sind herzlich eingeladen.