Dynamically Reconfiguring Hardware-Vulnerability Mitigations to Improve Energy Efficiency

Henriette Hofmeier
Ruhr-Universität Bochum (RUB)

Benedict Herzog
Ruhr-Universität Bochum (RUB)

Christian Eichler
Ruhr-Universität Bochum (RUB)

Stefan Reif
Ruhr-Universität Bochum (RUB)

Luis Gerhorst
Universität Erlangen-Nürnberg (FAU)

Timo Hönig
Ruhr-Universität Bochum (RUB)

Providing secure systems, for example, in computing centers, is an essential task of service providers. Vulnerabilities threatening secure execution are not only located in defective software but often also in hardware, for example, Meltdown/Spectre and Microarchitectural Data Sampling (MDS). As these vulnerabilities are often only partly fixable or even unfixable for already-deployed hardware, software and operating system developers go to great lengths to mitigate these attacks. However, software mitigations of hardware vulnerabilities come with considerable costs in terms of run time and energy demand for some applications. These overheads are tolerated to ensure secure execution, and the mitigations are typically active for the system's entire run time. Even though, due to differences in the data they handle and security concerns, in general, processes require varying degrees of protection. Thus, mitigations may only be required for short time spans or individual processes – if at all. However, current operating systems (e.g., Linux) lack such fine-grained control during run time.

In this talk, we present our ongoing research on dynamic and energy-aware reconfigurations of hardware-vulnerability mitigations within the Linux operating system. By adapting the mitigation configurations to the current workload and system state and selecting the best-suited mitigation, the system's performance and energy efficiency can be improved.