

Informatik–Kolloquium WS 2026/27

Donnerstag, 08.10.26, 15.15 Uhr, FAU Event Space
(Blaue Box), Freyeslebenstraße 1, 91058 Erlangen

Prof. Shweta Shinde

ETH Zürich

From Smartphones to Cloud: Trustworthy Foundations for Digital Sovereignty

As computing moves increasingly to the cloud and AI-powered services, a fundamental question emerges: who truly controls our data and computation? Today's systems force users to trust phone manufacturers, operating system vendors, and cloud providers, i.e., entities whose interests often conflict with user privacy and security. In this talk, I will present a research agenda to build systems that enable trustworthy sovereignty, where users can verify who controls their computation rather than blindly trusting cloud operators and management software.

I will demonstrate this vision by exposing and addressing trust failures across three critical architectural layers of modern computing. First, I'll show how we can enable users to reclaim control of their smartphones—running security-critical applications like encrypted messaging and password managers in isolation from both the operating system and manufacturer backdoors. Second, building such a system revealed a deeper problem: a new class of vulnerabilities that break the security guarantees of all major CPU-based trusted execution environments by exploiting fundamental assumptions about how processors handle hardware interrupts.

Finally, I'll expose an emerging attack surface in chiplet-based processors and accelerators used in the cloud: as components disaggregate, the interconnects linking them can be exploited to completely bypass security. To address this, I'll present techniques to systematically detect and prevent such vulnerabilities in hardware designs before chips reach production. Together, these contributions reveal fundamental vulnerabilities across the computing stack and demonstrate practical paths toward building systems where trust is verified rather than assumed, enabling genuine digital sovereignty for individuals, organizations, and nations.

Kontakt:

Prof. Dr. Rüdiger Kapitza
Informatik 4 (Systemsoftware)
www.sys.cs.fau.de