Guest Lecture

Reasoning about the trade-off between security and performance

Dr. sc. Boris Köpf
IMDEA Software Institute, Madrid

Tuesday, April 19, 2016
11:00 am - 12:30 pm
Room: Andreas-Pfitzmann-Bau 1004 (Großes Ratszimmer), Nöthnitzer Straße 46

Abstract: Today's software systems employ a wide variety of techniques for minimizing the use of resources such as time, memory, and energy. While these techniques are indispensable for achieving competitive performance, they can pose a serious threat to security: By reducing the resource consumption on average (but not in the worst case), they introduce variations that can be exploited by adversaries for recovering private information about users, or even cryptographic keys. In this talk I will give examples of attacks against a number of performance-enhancing features of software and hardware, and I will present ongoing work on techniques for quantifying the resulting threat and for choosing the most cost-effective defense.

Bio: After completing his Ph.D. in the Information Security group of ETH Zurich and working as a postdoc in the Information Security and Cryptography Group of the Max Planck Institute for Software Systems, Boris Köpf joined the IMDEA Software Institute Madrid and now holds an Assistant Research Professor position there. His research covers quantitative notions of security, techniques for computing corresponding guarantees for real systems, the analysis of side-channel attacks (and countermeasures), and privacy-preserving data publishing.