**Ahmad-Reza Sadeghi** ahmad.sadeghi@trust.tu-darmstadt.de

## A Hitchhiker Journey of Building and Attacking Secure Computing Systems

**Abstract:** The ever-increasing complexity of computing systems, emerging technologies such as IoT and AI, and advancing attack capabilities pose various (new) challenges to the design and implementation of security concepts, methods, and mechanisms for computing systems.

This talk provides a compact overview of our journey through the system security research universe. We point out lessons learned in advancing state-of-the-art software and hardware-assisted security in academic research and industry collaborations. We also briefly present our insights gained throughout the world's largest joint academic-industry hardware security competitions we have conducted since 2018. Finally, we discuss our future vision and new research directions in systems security, particularly in light of the severe threat of software-exploitable hardware vulnerabilities that put all critical systems at risk.

**Biography**

Ahmad-Reza Sadeghi is a professor of Computer Science and the head of the System Security Lab at the Technical University of Darmstadt, Germany. He has led several Collaborative Research Labs with Intel since 2012 and Huawei since 2019.

He has studied Mechanical and Electrical Engineering and holds a Ph.D. in Computer Science from the University of Saarland, Germany. Before academia, he worked in the R&D of IT enterprises, including Ericsson Telecommunications. He has been continuously contributing to the security and privacy research field. He was Editor-In-Chief of IEEE Security and Privacy Magazine and had been serving on the editorial board of ACM TODAES, ACM TIOT, and ACM DTRAP.

He received the renowned German "Karl Heinz Beckurts" award for his influential research on Trusted and Trustworthy Computing. This award honors excellent scientific achievements with a high impact on industrial innovations in Germany. In 2018, he received the ACM SIGSAC Outstanding Contributions Award for dedicated research, education, and management leadership in the security community and pioneering contributions in content protection, mobile security, and hardware-assisted security.

In 2021, he was honored with the Intel Academic Leadership Award at USENIX Security conference for his influential research on cybersecurity, particularly hardware-assisted security. In 2022 he received the prestigious European Research Council (ERC) Advanced Grant.