Title: Can't See the Forest for All the TEEs

Speaker: Moritz Schneider, Ph.D. student, ETH Zürich

Abstract:
The growing complexity of modern computing platforms and the need for strong isolation protections among their software components has led to the increased adoption of Trusted Execution Environments (TEEs). While several commercial and academic TEE architectures have emerged in recent times, they remain hard to compare and contrast. More generally, existing TEEs have not been subject to a holistic systematization to understand the available design alternatives for various aspects of TEE design and their corresponding pros-and-cons. In this work, we analyze the design of existing TEEs and systematize the mechanisms that TEEs implement to achieve their security goals, namely, verifiable launch, run-time isolation, cryptographic memory protection, trusted IO and secure storage. More specifically, we analyze the typical architectural building blocks underlying TEE solutions, design alternatives for each of these components and the trade-offs that they entail. We focus on hardware-assisted TEEs and cover a wide range of TEE proposals from academia and the industry. Our analysis shows that although TEEs are diverse in terms of their goals, usage models and instruction set architectures, they all share many common building blocks in terms of their design.

Bio:
Moritz Schneider is a Ph.D. student at the Institute of Information Security, ETH Zürich. His research interests include hardware security, trusted execution, and system security. Schneider received a MSc in electrical engineering from ETH Zürich.