Title: Application-oriented Security: Secrets Management and Side-Channel Protection for TEEs
Speaker: Christof Fetzer

Abstract: This tutorial will first introduce the problems one faces when trying to run unmodified applications inside of TEEs. Alternative solutions are presented but the focus will be on the use of cross-compilers and runtime support to execute applications inside of TEEs.
We will introduce some example applications running inside of SGX using the SCONE platform.

Second, we will motivate the need for integrating secrets management and remote attestation. We will motivate the problem of remote attestation and configuration management and show how to solve this. We show how that helps with transparent protection of files and secrets.

We show how attestation can help to protect against some side-channel attacks.
The main focus will, however, on a novel approach to protect against L1/L2-based side channels attacks.

Bio: Since April 2004, Christof Fetzer is a full professor and head of the Systems Engineering Chair in the Computer Science Department at Technische Universität Dresden.
He got his PhD from UC San Diego. He has been coordinating the H2020 projects SERECA (http://www.serecaproject.eu) and SecureCloud (https://www.securecloudproject.eu/) both aim at removing technical impediments to secure cloud computing. Both investigate the use of SGX to prevent adversaries with root access to read or modify application data and code.