TrustZone for ARMv8-A

Summary:

This course is designed to give platform developers a basic overview of designing trusted systems with ARM TrustZone Technology. The course will introduce the security extensions to ARMv8-A processors. Platform and software requirements to allow such operations as secure boot or DRM.

Prerequisites:

- Working knowledge of the ARM application processors
- Knowledge of programming in C
- Experience of programing in assembler is useful but not essential
- Knowledge of embedded systems

Audience:

Hardware and software system architects who need to understand the issues in developing trusted systems using the ARM TrustZone security extensions.

Length:

3 hours

Agenda:

- Security Overview
- TrustZone Memory Systems
- TrustZone Software Overview
- Exception Handling
- Secure Boot
- TrustZone Debug