TrustZone for ARMv8-A

Summary:

This live WebEx delivered course provides a technical introduction to designing trusted systems with ARM TrustZone Technology. It will introduce the security extensions to ARMv8-A processors and the platform and software requirements to allow such operations as secure boot or DRM. As well as hearing first hand from the engineer, you will also have the opportunity to ask questions to gain further specific knowledge on the subject

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