ARM TrustZone Technology Training

Summary:

This course is designed to give platform developers a complete overview of designing trusted systems with ARM TrustZone technology.

The course will introduce the privilege model and memory separation features of the v8-A architecture. It will discuss platform and software requirements to allow such operations as secure boot, DRM or Mobile Payment. The course discusses a complete trusted system including:

- Secure boot
- Secure monitor and EL3 Firmware
- Trusted kernel and applications
- Normal world OS drivers
- Platform design
- Memory protection

Prerequisites:

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

Audience:

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

Length:

3 days

Modules:

- Introduction to the ARM Architecture
- AArch32 Fundamentals (optional)
- Introduction to TrustZone Security
- TrustZone Hardware Overview
- TrustZone Software Overview
- TrustZone Memory Management
- TrustZone Exception Handling
- Programming the GIC (Generic Interrupt Controller)
- Virtualization
- Programming the System MMU (Optional)
- TrustZone Secure Boot
- TBBR and Trusted Firmware
- TrustZone Software Stack
- TrustZone System Architecture
- TrustZone Debug
- TrustZone Ecosystem