1 Implementing a ARM-based Secure Boot Scheme for the Isolated Execution Environment

1.1 Introduction

All the secure isolation based applications are based on the assumption of a secure execution environment. However, the isolation environment created by TrustZone is not a complete secure environment. It is possible that the device is attacked during start-up process. If the attacker modifies the system image in the external memory and obtains system privileges, the security of applications in the attacked system will be unknown.

1.2 Design and Implementation

The execution environment of TrustZone is an isolated execution environment rather than trusted. In order to build a truly trusted execution environment, secure boot is adopted through structuring root of struct and trust chain which ensures the device boot is secure.

Boot sequence

1. Device Power On
2. BootROM
3. First Stage BootLoader (FSBL)
4. U-boot
5. OP-TEE Kernel
6. Linux Kernel
7. System Running

Building Root of Trust The BootROM performs RAS authentication, AES decryption and HMAC authentication in sequence to check FSBL for tampering or being attacked. The keys for these algorithms during secure boot are saved in eFuse arrays on the board. After device is power-on or reset, the on-chip BootROM begins to perform CRC for its own integrity, it loads the FSBL into memory and compares the SHA signature of the boot image with the stored hash value. If all authentications have passed, the control will be turned over to the decrypted FSBL.

The trust chain The device could build a trust chain through validation of each stage, and it ensures that the execution environment is trusted. At each boot stage, the image of the next stage should be verified. This way the entire trust chain is being built, if verification of every stage is succesfull the device is booted up securely.