1 Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes

1.1 Introduction

IoT devices suffer from Hardware attacks, OS/Firmware attacks and software attacks. All of these attacks damage the integrity of the IoT system. In order to enforce a strong system integrity policy, ARM TrustZone technology is leverated to ensure both the load-time integrity and the runtime integrity of the IoT system. The Root of Trust (RoT) is created through secure boot, this is how the load-time integrity will be assured. The runtime integrity is achieved through periodically attesting the normal world by the secure world in a paged manner.

1.2 Threat Model

We assume that attackers have physical access to IoT devices. They can launch hardware attacks, OS/firmware attacks and software attacks against IoT devices. Before the IoT devices are powered up, the attackers can tamper with the firmware images of both the SW and the NW stored in the flash memory. During system runtime, the attackers can inject malware in the NW and tamper with NW built-in programs arbitrarily. Only the security of the code section of a program is considered.

1.3 Hybrid Booting Approach

Root of Trust As the trusted base for the hybrid boot, the RoT is first established based on the OCROM and eFuse. The OCROM is a read-only memory with write-protection, the on-chip eFuse is a one-time-programmable (OTP) electronic element, whose contents cannot be modified once programmed. Therefore, the OCROM and the eFuse are leveraged as the system RoT since both are immune to being tampered with. The first-stage bootloader is stored in the OCROM, responsible for verifying the integrity of the second-stage bootloader using a public key. The hash of the public key is stored in the eFuse and used to verify the public key's integrity.

Secure Boot Secure boot is used to start the SW and ensure the integrity of it. The secure boot involves two phases, the offline image signing phase and the online secure boot phase. The second-stage bootloader image and the secure OS kernel image are measured and signed offline. A hash of the second-stage bootloader image is calculated and used as its measurement result. A CoT can be established based on the first-stage bootloader. On powering up, the first-stage bootloader acts as the trusted base of the secure

boot. It passes the control to the second-stage bootloader after successfully loading and verifying the integrity of the second-stage bootloader, and so on.

Trusted Boot After the secure OS kernel gets started, trusted boot is used to boot up the NW to ensure its integrity. The trusted boot for the NW involves two phases: the offline hash chain calculation phase, and the online trusted boot phase. Furthermore, the remote attestation key needs to be securely stored in the flash memory.

1.4 Paging-based Process Integrity Measurement and Attestation Method

Offline measurements on the code sections of the pre-installed programs at the page granularity level can be performed in the NW and the measurement results as reference values can be stored on the remote attestation server. Then the code segments of the runtime processes residing on the memory page can be measured using a measurement TA in the SW, and finally the results can be sent to the remote attestation server to verify the integrity of processes.

1.5 Evaluation