Advances in Artificial Intelligence, Big Data and Algorithms
G. Grigoras and P. Lorenz (Eds.)

doi:10.3233/FAIA230876

Secure Startup Scheme for Asymmetric Embedded Software Based on Multiple Cores

Fang YUAN[1], Dejian LI[2], Xi FENG[3], Bin NIU[4]
Digital Chip Design Center, Beijing Smart-chip Microelectronics Technology Co., Ltd., Beijing 100192, China

Abstract—Aiming at the real-time requirement of relay protection device, a secure startup mechanism of multi-core asymmetric software was proposed based on a self-developed chip with two clusters and four cores of ARM Cortex-A53 processor, which could meet both the security requirements of embedded devices and the real-time requirements of relay protection device. The overall design idea, security hardware protection module and software architecture of the mechanism are described, and the security is analyzed in detail. Experiments show that the proposed scheme can be used as a trusted system to measure the integrity of embedded devices, so as to realize the secure startup of embedded devices.

Keywords-Embedded system, Secure startup, Trust root, Trusted startup, Multi-core asymmetric software

1. Introduction

With the development of embedded technology, in view of the embedded intelligent terminal security has also been more and more attention. Trusted startup is the foundation of all system behavior, not only load during startup code itself, is responsible for the initialization of an embedded equipment physical device and the state of the system itself, allocate memory and hardware and software resources, etc., also start the system of service and necessary to sustain the normal operation of all kinds of process, Including secure and trusted processes. Any error during startup can cause the operation of an embedded device to enter an unpredictable and dangerous state. Trusted Computing Group (TCG) has promoted the development of trust computing technology by applying trust root and trust chain technology. Many subsequent studies are also focused on the Trusted Platform Module (TPM) of trusted computing platform [1]. Researchers from Nanrui Group have designed their own security module using OTP

[1] Corresponding Author: Fang YUAN, Digital Chip Design Center Beijing Smart-chip Microelectronics Technology Co., Ltd.; e-mail: yuanfang@sgchip.sgcc.com.cn
[2] Dejian LI, Digital Chip Design Center Beijing Smart-chip Microelectronics Technology Co., Ltd.; e-mail: lidejian@sgchip.sgcc.com.cn
[3] Xi FENG, Digital Chip Design Center Beijing Smart-chip Microelectronics Technology Co., Ltd.; e-mail: fengxi@sgchip.sgcc.com.cn
[4] Bin NIU, Digital Chip Design Center Beijing Smart-chip Microelectronics Technology Co., Ltd.; e-mail: niubin@sgchip.sgcc.com.cn

chip as trusted root for specific interface, [2] but this undoubtedly increases the burden of embedded system hardware and software system.

Therefore, ARM proposed a hardware level mobile platform security technology TrustZone [3], through the processor core unit, system bus, peripheral devices, memory, cache registers and other hardware security expansion, CPU chip is the system "trusted root". At present, embedded terminals are developing rapidly and there are many kinds. The research of this paper is based on a chip developed by ARM Cortex-A53. The software architecture of the system is also based on the strong real-time requirements of industrial systems such as power systems. The Asymmetric multi-core (AMP) structure is adopted instead of the commonly used Symmetric multi-core Symmetric Multi-Processing (SMP) [4].

2. Design and Implementation of Multi-Core Asymmetry

2.1.Security Hardware Introduction

The security hardware construction of the scheme mainly includes the following aspects：

- Core-level ARM Trustzone establishes a multi-level execution environment for trust security requirement services
- Cryptography Engines includes Crypto engines (Cipher/HASH), TRNG, Embedded DMA for transfer data between DDR and WTM, FUSE Burning Interface.
- TZC400 is used for SOC Sub-System access permission control
- Secured FUSE module for boot and system usage.
- On-chip BootROM image as the Platform Root of Trust for Secure Processors to boot up from.

2.1.1 TrustZone. TrustZone is a security architecture solution provided by ARM, which provides a secure hardware foundation for embedded systems and has been widely recognized in the industry[4]. TrustZone implements the mechanism through the hardware structure, divides the storage into safe and non-safe areas[5], and accesses it through the Cryptography Engines.[6]

2.1.2 Cryptography Engines. The Cryptography Engines unit can be instantiated either in FIPS 140-2/3 compliant mode, or in Non-FIPS (accelerator-only) mode. The FIPS mode utilizes a Hardware-Root-Of-Trust authorization scheme for authenticating the use of keys and provides the basis for secure, trusted operations. The FIPS mode contains intelligence in the form of firmware and behavior documented herein.

2.1.3 TZC400. The TZC400 operates between ACE-Lite masters and ACE-Lite slaves in a TrustZone system and filters bus accesses from masters to slaves.It performs the filtering based on security requirements that are specified for address regions. You can program the eight TZC-400 address regions with varying security requirements for your intended application.You can program the TZC-400 to report faults using the ACE-Lite response channel or interrupts. Figure 1 shows a high-level view of the TZC-400 with a control unit and between one and four filter units.

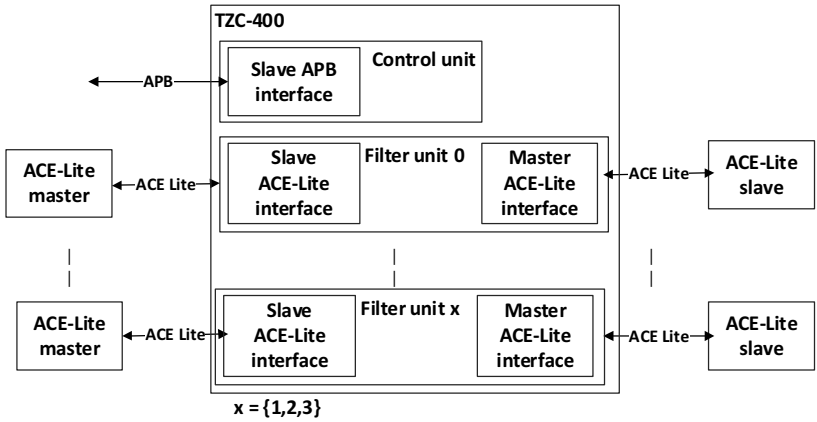

Figure 1. TZC400 overview

2.1.4 FUSE. This scheme uses TSMC HD FUSE measured in bank(256 bit) as unit, will burn one bank at every burning action, but while perform read action will update all banks' value. TSMC FUSE module has 32 bit wide data port, hardware FSM will shift all fuse value out[7]. This scheme uses double bits mode. The same data bit is stored in both fuse macro 0 and fuse macro 1. The final data is obtained by an "OR" operation of values from both macros with the same address. That means while fuse burning, for every fuse bank, we need burn twice with the same fuse value. This scheme further ensures that the data is not tampered with as shown in Figure 2

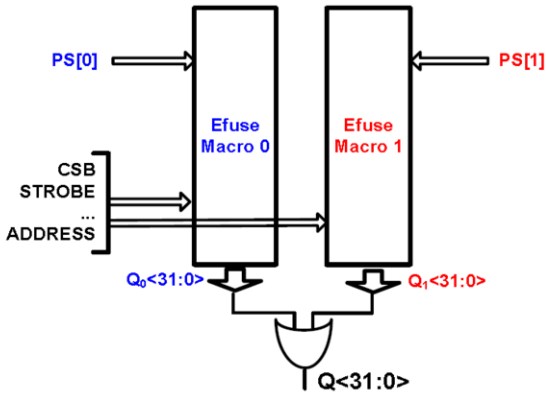

Figure 2. FUSE Dual Bit Mode

2.2.Multi-core Asymmetric Software

In order to meet the real-time requirements of the relay protection device, this paper designs the asymmetric software architecture as shown in Figure 3, and allocates hardware and memory resources for different systems in the start-up stage.linux is used to meet the requirements of multiple applications, while these strong real-time applications runs in baremetal.

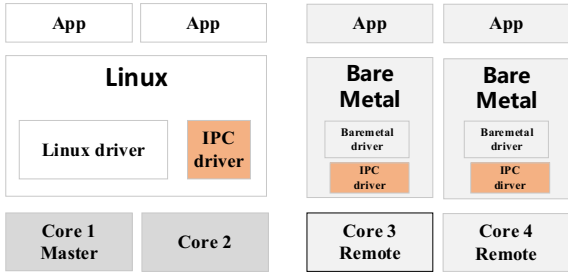

Figure 3. Asymmetric software frameworks

3. Secure Startup Design of Multi-Core Asymmetric Embedded Software

The purpose of safe startup is to ensure that the content of each stage of the system is safe during the startup process. In other words, it adopts the form of trust chain and realizes the chain transfer of trust through the integrity verification of modules at all levels. Since BootRom is written in a single time during the chip production stage, it does not allow erasable or repeated writing, which provides an absolutely trusted trust root for the chip. Core0 in Cluster0 as the master core is booted from BootRom as shown in the figure 4.

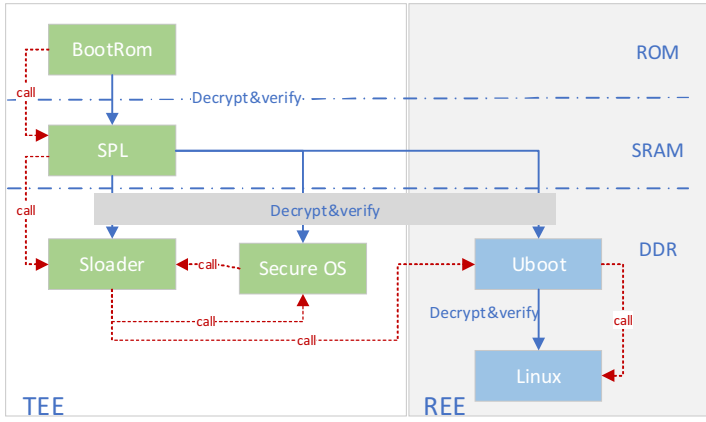

Figure 4. security start-up of master core

The BootRom starts execution from the TEE environment. SPL is loaded into SRAM by BootRom to run, the DDR is initialized, and then Sloader, Secure OS and uBOOT are loaded into the DDR. After loading, execution is transferred to Sloader. After the Secure OS is initialized by Sloader, the execution is transferred to Uboot. After entering Uboot, the system switches to the REE environment. After Uboot loads Linux into DDR, the execution transfers Linux and finally executes to the Linux Shell. The BootRom is responsible for decrypting or verifying the SPL. The SPL is responsible for decrypting or verifying the signature of Sloader, Secure OS, and Uboot. Uboot is responsible for decryption or signature verification of Linux, and the relevant decryption and signature verification process will be completed through the interface of SMC into the TEE environment (Secure OS).[8][9][10]

These ensure that the chip has an absolutely secure root of trust boot.

The real startup process is shown in Figure 5，The safe startup process of the whole system is as follows:

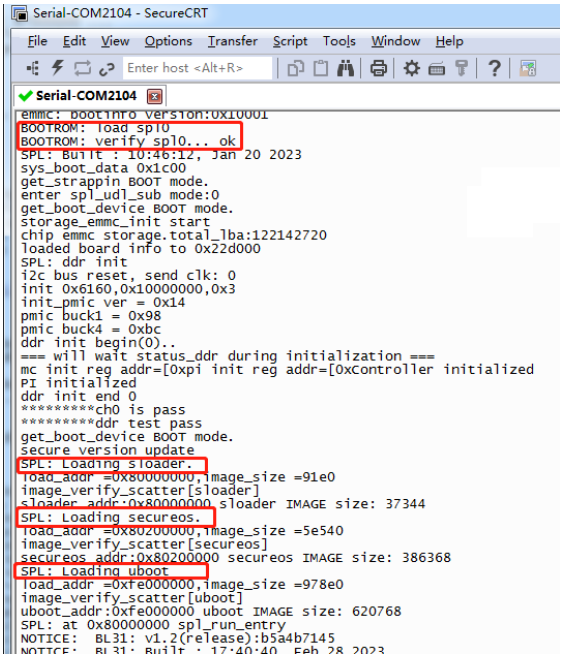

Figure 5. the real startup process

In addition, as a multi-core and multi-system chip, a safe and credible trust chain not only involves the startup process of a software system, but also the safe transfer between cores is also crucial. Figure 6 shows the safe transfer and verification step by step between multiple cores, which ensures the startup safety of the whole chip [11]. When the main core is powered on and started from BootROM, other cores enter the WFE state under the guidance of SPL and wait to be loaded the code and be started.

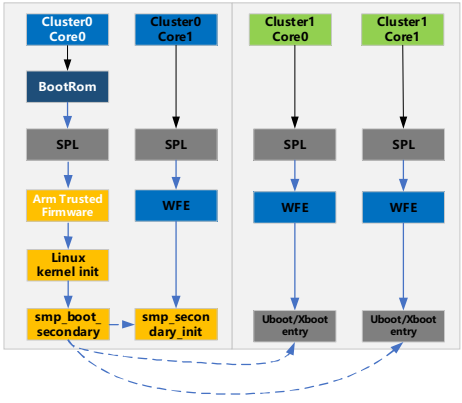

Figure 6. Multi-core security start-up framework diagram

4. Process Integrity Verification for Multi-Core Asymmetric Embedded Software

In order to verify whether the restarting mechanism can effectively resist tampering and attacks, two verification scenarios are designed here:

- Verify that when the master core firmware is modified, the startup process can be normally identified and the startup is terminated
- Verify that when the slave core firmware is modified, the boot process can correctly identify and terminate the boot of the slave core.

Verify scenario one, as shown in Figure 7, contains the correctly signed kernel image and the master core linux can boot normally.

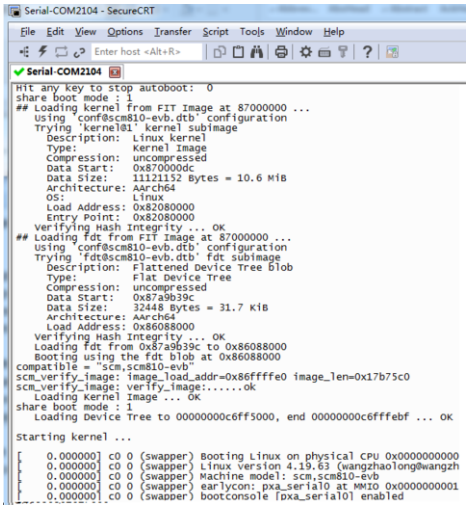

Figure 7. the master core starts normally with correctly signed kernel

At the same time, on the basis of the original, a piece of uboot code is tampered, the kernel image is generated, the image is re-burned, and the experiment board is started. The boot information can be seen from the serial port debugging tool, as shown in Figure 8. After the boot file is penetrated, the boot process verification fails and the boot is terminated.

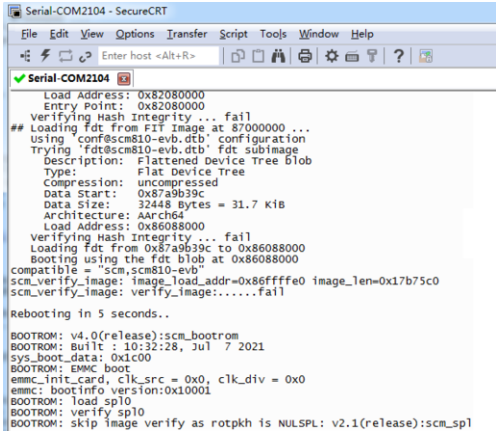

Figure 8. Validation failure of modified kernel image

To verify scenario two, as shown in Figure 9, the correctly signed baremetal.img can start normally and respond to the interrupt normally under the control of the master core linux.

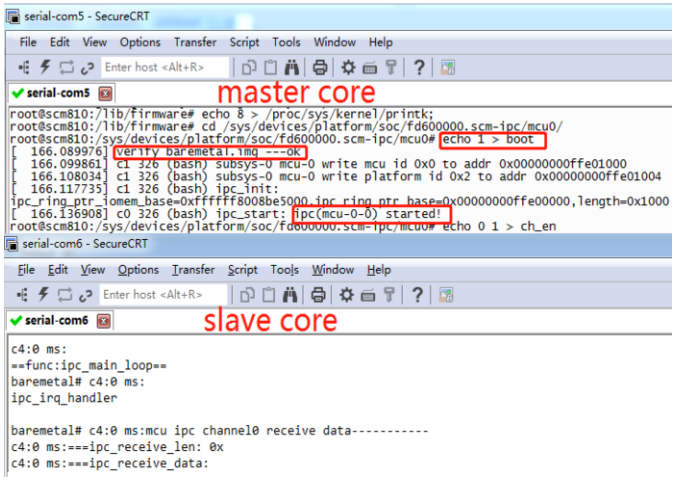

Figure 9. the slave core starts normally with correctly signed baremetal image

At the same time, when the master core linux starts the tampered slave core code baremetal.img, the boot process fails to pass the verification and the boot is terminated. As shown in Figure 10.

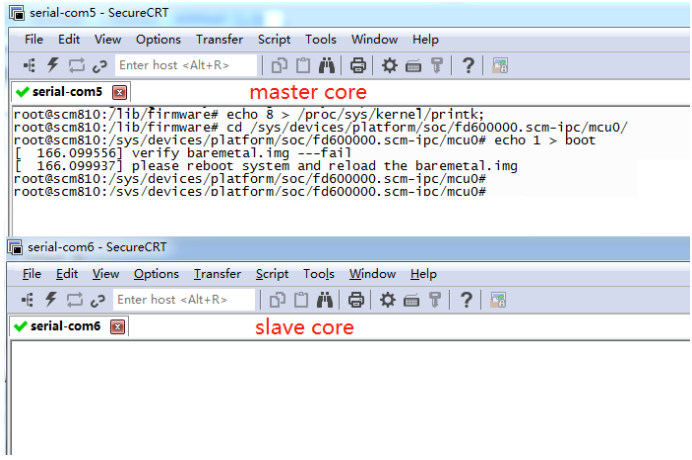

Figure 10. Validation failure of modified baremetal image

5. Conclusions

In this paper, from the perspective of solving multi-core secure boot, we study a software secure boot scheme based on ARM Trustzone, which meets the security requirements of multi-core boot to a certain extent, but it needs to be further improved.

Acknowledgments

This paper is funded by the project of the State Grid Corporation of China in 2021, "Key verification technology research and IC development for high end controller chip （5700-202141255A-0-0-00）"

References

[1] Wang X, Xu G, Han Y , rt al. A trusted conputing architecyure of embeded system based on improved TPM. In: Proc.of the MATEC Web of Conf on EDP Sciences, Vol.139.2017
[2] Trusted Computing Group.TCG Mobile Trusted Module Specification.Version 1.0. 2007
[3] FAN Guannan, DONG Pan. Research on Trusted Execution Environment Building Technology Based on TrustZone[J].Netinfo Security, 2016 (3) : 21-27.
[4] Jiri Hlusi. Symmetric Multi-Processing(SMP) systems on top of contemporary Intel appliances[D]. University of Tampere Department of Computer and Information Sciences, December 2002.
[5] ARM. ARM Security Technology-Building a Secure System Using TrustZone Technology[EB/OL]. http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.prd29-genc-009492c/index.html, 2015-6-12.
[6] Sandeep G. An edge-computing based Industrial Gateway for Industry 4.0 using ARM TrustZone technology[J]. Journal of Industrial Information Integration,2023,33.
[7] Ahmad W B. FUSE based file system for efficient storage and retrieval of fragmented multimedia files[J]. Journal of King Saud University - Computer and Information Sciences,2022,34(10PA).
[8] ARM Company. CoreLink™ TrustZone Address Space Controller TZC-380[EB/OL]. Technical Reference Manual, 2009.
[9] ARM.TrustZone [EB/OL]. http://www.arm.com/zh/products/processors/technologies/trustzone/index.php,2015-8-23.
[10] ARM Company. SMC CALLING CONVENTION System Software on ARM® Platforms[EB/OL]. Technical Reference Manual, 2014.
[11] 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Trusted Execution Environment: What It is and What It is Not. Helsinki, Finland., 2015-12-18.