The road to BIOS development (Part 3) - the concept and startup phase of UEFI

原创 Practitioner xxl Modified on 2024-09-14 13:41:45 Read 2.7k Collection 38 Likes 28
Category columns: BIOS Development Article Tags: server C++ Embedded Hardware

Copyright CC 4.0 BY-SA

BIOS Development This column includes this content 26 articles Subscribe to our column

1. UEFI Overview

1. UEFI stands for Unified Extensible Firmware Interface, which defines the interface between the operating system and platform firmware. It allows the PC to load the operating system from the pre-boot operating environment and is a replacement for BIOS. The interface UEFI provides to the operating system includes boot-time services and runtime services.

2. Improvements of UEFI over BIOS:

(1) UEFI supports more hardware than BIOS. UEFI can use a hard disk larger than 2.2TB as a boot disk, while BIOS can only be used as a data disk without the help of third-party software.

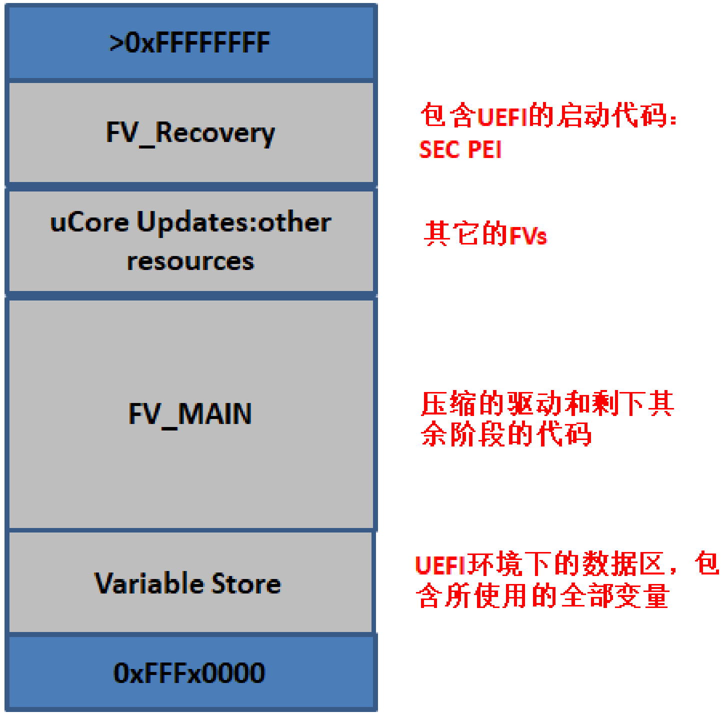
(2) UEFI provides a high-resolution graphical interface. Once the user enters the interface, they can use the mouse to make settings and adjustments just like in an operating system, which makes the operation simpler and faster.

(3) UEFI mostly uses C language instead of assembly language, and adopts a modular design. It can be logically divided into two parts: hardware control and software management. The former uses standardized universal settings, while the latter is a programmable open interface. Therefore, i motherboard manufacturers can use the open interface to implement a variety of rich functions on their own products, including screenshots, data backup, hardware fault di
operating system.

3. Composition of UEFI Flash ROM

UEFI's Flash ROM firmware consists of one or more Firmware volumes (FVs), each of which stores FFS Images (EFI Firm
multiple EFI Sections, which contain PE32/PE32+/Coff Image files. The memory mapping of UEFI firmware is as follows:

After logging in, you can enjoy the following benefits:
Free Copy Code
Interact with bloggers
Download massive resources
Post updates/write articles/join the community
Sign in now


>0xFFFFFFFF
FV_Recovery
包含UEFI的启动代码：
SEC PEI
uCore Updates:other resources
其它的FVs
FV_MAIN
压缩的驱动和剩下其余阶段的代码
Variable Store
UEFI环境下的数据区，包含所使用的全部变量
0xFFFx0000

UEFI Flash内存映射

CSDN @修行者xx

2. UEFI composition and startup phase

UEFI is mainly composed of initialization module, driver execution environment, driver, compatibility support module, UEFI application and GUID disk partition. The initialization module and driver execution environment are the basis of UEFI operation and are usually integrated into the flash memory chip of the motherboard. The startup of UEFI can be divided into seven stages. The first three stages are the CEFI initialization stage, and the last four stages are the operatin

×

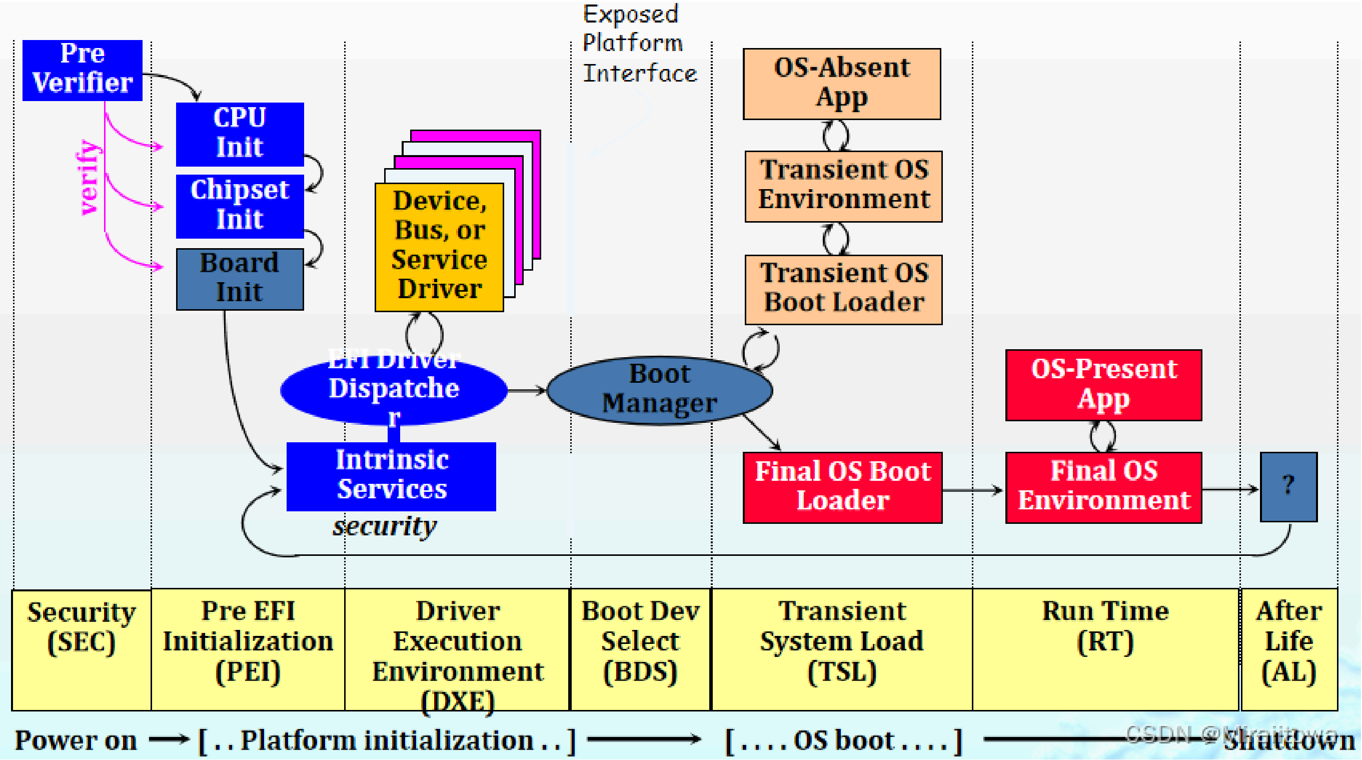
After logging in, you can enjoy the following benefits:

Free Copy Code

Interact with bloggers

Download massive resources

Post updates/write articles/join the community



1. SEC (Security Phase)

SEC is the starting point of the entire system. The computer enters this stage first after power-on. It mainly does four things:

(1) Receive and process system startup, restart, and abnormal signals.

(2) In the SEC phase, only the CPU and CPU internal resources are initialized. Various external devices and memory are not initialized. Therefore, the system needs a part of temporary memory for code and data storage, called temporary RAM (volatile) , which is located inside the CPU. The most c is generally composed of SRAM, and the arithmetic unit, controller, memory, and cache are all encapsulated inside the CPU.

(3) SEC is the root of the trusted system. Only when it is trusted by the system at the SECX stage can the following stages h

(4) Control is transferred to the next stage PEI phase, passing system parameters, including: the address and size of the sta system, the address and size of the bootable firmware, and the address and size of the temporary RAM area.

The SEC's execution process is shown in the figure:

×
After logging in, you can enjoy the following benefits:
Free Copy Code
Interact with bloggers
Download massive resources
Post updates/write articles/join the community

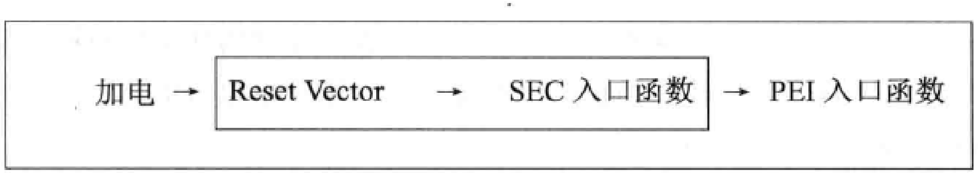


图 1-3 SEC 阶段执行流程

CSDN @修行者xxl

The execution of SEC is divided into two parts, with the temporary RAM initialization as the boundary: the Reset Vector phase before the temporary RAM takes effect, and the SEC entry function is called after the temporary RAM takes effect to enter the SEC function area. How to execute the BIOS program when the computer starts

2. PEI (Pre-EFI Initialization)

The PEI stage initializes the memory. Its main function is to prepare the execution environment for the DXE stage, compose the HOB list with the information that needs to be passed to DXE, and transfer the control to DXE.

(1) Initialize the memory so that it can be used.

(2) Prepare the execution environment for the DXE stage: basic chipset initialization, memory sizing, BIOS recovery, S3 resume, switch stack to memory, and start DXEIPL.

HOB (Hand-Off Block) is a data structure used in the PEI stage. Its main functions are as follows:

1. Data transfer: HOB is used to transfer data between modules in the PEI stage. Since memory management has not been fully established in the PEI stage, HOB provides a mechanism that allows different PEIMs (PEI modules) to share data and information.

2. Resource description: HOB can describe system resources, such as memory, devices, ACPI tables, etc.

3. Build memory map: An important task in the PEI stage is to build memory map. HOB is used to record the type, size and attributes of memory to help build the system's memory map.

4. System configuration: HOB can contain system configuration information, such as firmware settings, BIOS settings, etc. Th system in the subsequent stage.

5. Boot parameters: HOB can contain boot parameters, which affect the system startup behavior, such as boot device selecti

6. Prepare for the DXE stage: After the PEI stage, the HOBs will be passed to the DXE stage. The initialization code of the D the system and load the necessary driver information.

】

×
After logging in, you can enjoy the following benefits:
Free Copy Code
Interact with bloggers
Download massive resources
Post updates/write articles/join the community

3. DXE (Driver Execution Environment) driver execution environment stage

The DXE stage performs most of the system initialization work. When entering this stage, there is enough memory available, so a lot of driver loading and initialization work is completed. The System Table is generated to provide services for each stage. Control is given to BDS.

4. BDS (Boot Device Select) boot device selection phase

Initializes the console device (the physical hardware device that allows the user to interact directly with the computer system. It includes components such as the keyboard and monitor) , loads the necessary drivers, and executes startup items based on user selections.

5. TSL (Transient System Load) operating system loading early stage

TSL is the first stage of the OS Loader execution. It prepares the execution environment for the OS Loader and is called a temporary system. It has the prototype of the OS. UEFI Shell is the interactive interface of the temporary system. UEFI Shell will be entered when manual intervention or serious problems occur in the OS Loader.

In the TSL stage, system resource management is managed by BS. The services provided by BS include: time service, memory management: memory management and release, management system memory mapping, Protocol management, Protocol utility services, driver management: connect service for installing the driver to the controller, and disconnect service for uninstalling the driver from the controller, image management, and ExitBoolServices.

6. RT (Run Time)

The operating system loader obtains control of the system and recycles and cleans up the resources occupied by UEFI. The services provided include: time service, reading and writing UEFI system variables, virtual memory service and other services. If errors and exceptions occur at this stage, AL will be entered for repair.

7. AL (After Life) Disaster Recovery Phase

If the system (hardware or software) encounters a catastrophic error in the RT phase, the system firmware needs to provide error handling and disaster recovery mechanisms, which run in the AL phase. Based on the manufacturer's customized repair solution, neither UEFI nor UEFI PI defines the behavior and specifications of the AL phase.

Reference article link: https://blog.csdn.net/weixin_73231980/article/details/132336491

用Scrapy给TikTok喂"流量兴奋剂"

逆向工程竞品标签池：3天霸榜技术流→ 技术人优先预约通道

After logging in, you can enjoy the following benefits:

Free Copy Code
Interact with bloggers
Download massive resources
Post updates/write articles/join the community

©1999-2025 Beijing Innovation Lezhi Network Technology Co., Ltd.

×

After logging in, you can enjoy the following benefits:

Free Copy Code Interact with bloggers

Download massive resources Post updates/write articles/join the community