EFI (и UEFI)

Свитков Сергей
группа 344

СПбГУ

6 мая 2017 г.

Введение

Что же такое EFI?

- Extensible Firmware Interface
- Спецификация интерфейса, разделяющего аппаратный слой и слой операционной системы
- Разработка Intel
- Используется для загрузки установленных операционных систем
- Пришло на замену устаревшему BIOS
- На самом деле, само уже успело устареть (с 2005)

Немного истории

- Первоначальные идеи возникли при разработке Intel Itanium
- Изначальная мотивация — замена BIOS, обладающего тонной недостатков
  - 16-bit processor mode
  - 1MB адресуемой памяти
  - Завязано на IBM PC/AT
- Первые шаги разработки EFI были предприняты в 1998 (тогда название было иным: Intel Boot Initiative)
- В июле 2005 передали разработку UEFI Forum, поэтому EFI -> UEFI
- Последняя версия спецификации UEFI — 2.6, январь 2016

Преимущества по сравнению с BIOS

- Поддержка GPT, как следствие — возможность загрузки с дисков с объемом > 2TB
- CPU-Independent архитектура
- CPU-Independent драйвера
- Гибкая pre-OS среда (в т.ч. поддержка связи с интернетом)
- Обратная совместимость

Совместимость

Совместимость с процессорами

- Itanium, x86, x86-64, ARM (AArch32), ARM64 (AArch64)
- В отличие от BIOS поддерживает 32 и 64 режимы
  - Позволяет приложениям, работающим до загрузки системы, получать доступ ко всей памяти
- Разрядность процессора и разрядность ядра должны совпадать
- Возможность загрузки 64-битного ядра на 32-битной реализации UEFI, запущенной на x86-64 CPU

Совместимость

Совместимость с дисками

- Поддержка и MBR и GPT
- MBR ограничивает количество разделов (до 4х на диске) и их размер (до 2 GB)
- В GPT таких ограничений нет (на самом деле есть ограничение на размер разделов до 2^{73} байт)

Совместимость

Совместимость с Linux

- Поддержка GPT осуществляется включением опции CONFIG_EFI_PARTITION при настройке ядра
- Можно использовать GPT и в BIOS-based системах с помощью BIOS-GPT (в GRUB 2)
- При желании можно добиться этого и в GRUB, но не будем об этом (Серьезно, кто использует первый GRUB в 2017?)
- UEFI-системы могут использовать UEFI-методы загрузки, в таком случае загрузка осуществляется с ESP
- Для обратной совместимости есть поддержка MBR

Совместимость

Совместимость с windows

- Есть поддержка начиная с Windows Vista

Features

Сервисы

- Определяются два типа сервисов:
  - boot services: доступны только до тех пор, пока аппаратный слой управляет платформой. Включают поддержку терминалов, а так же сервисы шины, блокировки и файлов
  - runtime services: доступны при работе ОС; включают сервисы даты, времени и доступ к NVRAM
- Variable services: предоставляют возможность сохранения данных, которые могут быть использованы и ОС и железом
- Time services: предоставляют поддержку временных зон, что позволяет установить аппаратные часы на UTC или локальное время

Features

Приложения

- Перед загрузкой ОС UEFI может запускать UEFI-приложения.
- Например, загрузчики ОС: refind, GRUB (GRUB 2), systemd-boot
- Можно предоставить возможность запуска других приложений

Features

Протоколы

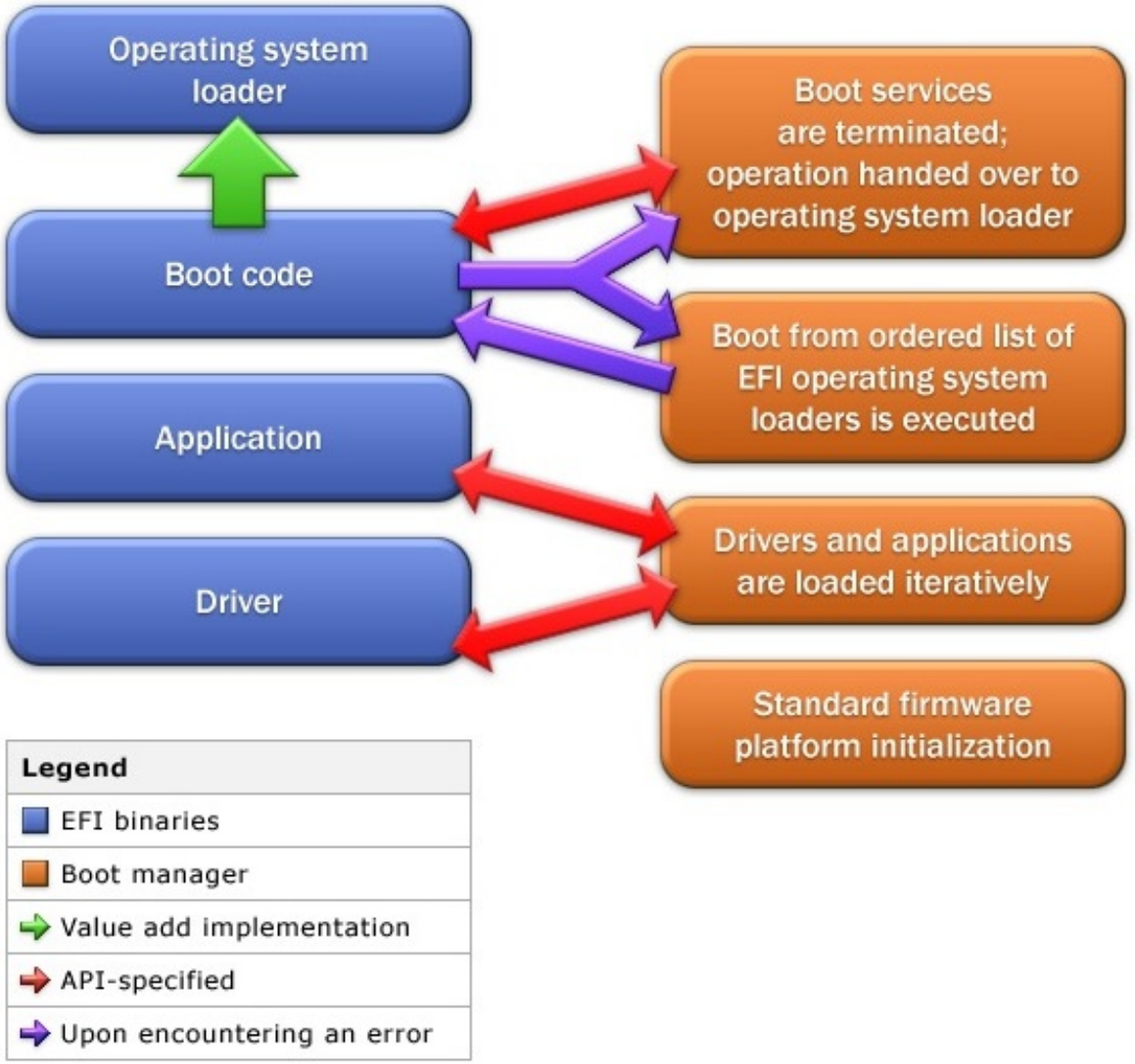
- Поддерживает набор протоколов для коммуникации
- UEFI-драйвера должны предоставлять сервисы с помощью протоколов

Драйвера устройств

- Помимо стандартных драйверов, специфичных для архитектуры, EFI предоставляет CPU-Independent драйвер устройства
- Хранится в памяти в EBC (EFI Byte Code)
- Можно поддерживать и специфичные для архитектуры драйвера, это позволит использовать графику/интернет до загрузки ОС-драйверов

Features

Взаимодействие между EFI-bootmanager’ом и EFI-драйверами



Features

Графика

- EFI использовало UGA-протокол (Universal Graphic Adapter) для поддержки графики
- UEFI использует Graphics Output Protocol с целью избавиться от зависимости от VGA
- Большинство ранних реализаций были основаны на CLI, но с 2007 появилась поддержка GUI

Features

EFI system partition

- Хранит UEFI-applications и файлы, которые нужны приложениями (например, ядро вашего дистрибутива)
- В качестве ФС используется специальная версия FAT
- Есть место для boot-sector для обратной совместимости с BIOS

Features

Загрузка

- UEFI-booting
  - Использует не boot sector, а boot manager
  - Автоматически распознает загрузчики ОС
- CSM (Compability Support Module) booting — для обратной совместимости
- Network booting
- Secure boot
  - Специальный протокол, который не позволяет загружаться драйверам или загрузчикам ОС с неподходящей сигнатурой

Features

UEFI shell

- Shell environment
- Позволяет запускать различные UEFI-приложения
- Может быть полезен для исправления/диагностики проблем с загрузчиками