Исполняемые файлы. Загрузка ОС

6#АКОС 2019-2020

Стадии компиляции

1. Создание объектных файлов
2. Компоновка **исполняемого файла**

Современные форматы исполняемых файлов x86

- Flat-form binary - без заголовков
  .com .sys в DOS/CP-M, загрузчики
- Executable and Linkable Format (ELF)
  используется в большинстве UNIX-систем
- Mark Zbykowski Portable Executable (MZ PE)
  используется в Windows
- Mach-O
  яблоки

ELF

- Начинается с magic-bytes {0x7F, 'E', 'L', 'F'}
- Далее - бинарный заголовок:
  - архитектура процессора
  - разрядность файла и процессора
  - entry point
  - положение сегментов описания

Демонстрация elftools.elf.elffile

Интерпретатор ELF

- Программа, которая реально запускается для загрузки и размещения в памяти
- Выполняет поиск всех зависимых библиотек
- Загружает в память библиотеки и сам файл
- Выделяет память на стеке
- Передает управление на entry point

Где искать библиотеки?

- Конфиг /etc/ld.so.conf
- Переменная окружения LD_LIBRARY_PATH
- Секции DT_RPATH и DT_RUNPATH в файле

- gcc -Wl,-rpath,КАТАЛОГ
  Можно использовать подстановки:
  - $ORIGIN - каталог программы
  - $PWD - текущий каталог
  - $LIB - имя lib или lib64
  - $PLATFORM - то, что выдает команда arch

Демонстрация: компиляция с библиотекой в rpath

Что такое "динамическая библиотека"

- Формат ELF-файла один для выполняемых файлов и библиотек
- И выполняемом файле есть **точка входа**
- В библиотеке есть **таблица символов**

Демонстрация: компиляция файла как в библиотеку, так и exec

DOS и Windows

- Mark Zbykowski Portable Executable (MZ PE)
- Аналогичен старому UNIX-формату COFF
- "Portable" означает несколько заголовков файлов: DOS, Win32, .NET
- Не использует позиционно-независимый код:
  - у каждой библиотеки есть базовый адрес загрузки в память
  - для стандартных библиотек адреса уникальны
  - на случай перекрытия - Relocation Table для каждой секции

Демо: проблема с Wine при ограничении VMSize

Flat-Form Binary

- Никаких заголовков
- После загрузки файла - call на его начало
- Последняя инструкция в файле - ret

- Обычно используется в реальном (16-битном) режиме процессора. Под адресом начала подразумевается значение регистра CS

Реальный режим процессора x86

- Процессор стартует в этом режиме
- Размер адресного пространства - 1Мб, из них под RAM - только 640Кб
- Вся память делится на сегменты по 64К
- Адреса начала сегментов хранятся в:
  - CS - сегмент кода
  - SS - сегмент стека
  - DS - сегмент данных

1MiB адресного пространства

0xFFFFF	1Mb above
0xC0000	ROM: • Video BIOS (32K) • Hardware BIOS (160K) • BIOS (64K)
0xA0000	VGA Shadow 128K
0x00000	RAM 640K

- Адресное пространтсво, доступное в реальном режиме процессора
- «640К хватит всем!» (с) Билл Гейтс
- VGA Shadow - только для текста
- ROM - код программ
- i80286 процессоры имеют разрядность 24 бит, а не 20 бит

Программные прерывания

- Команда int NN
- С точки зрения обработки ничем не отличаются от аппаратных

- До загрузки ОС - функции BIOS
- ОС может (но не обязана) модифицировать таблицу прерываний

Некоторые прерывания

В AH хранится команда, в AL - аргумент

BIOS

- INT 0x10 - управление текстом на экране
- INT 0x13 - управление дисками
- INT 0x15 - управление UART
- INT 0x16 - опрос клавиатуры
- INT 0x17 - опрос клавиатуры

DOS

- INT 0x21 - взаимодействие с DOS API

Стадии загрузки на x86

THE KERNEL И ЕГО ЗАГРУЗКА

Ядро операционной системы

- Программа операционной системы, которая запускается первой
- Работает на привелигированном уровне

Демо: файлы ядра Linux и Windows

Загрузчик

- Должен найти каким-то образом файл на диске
- Загрузить его штатным образом как обычную программу
- Запустить

Классический PC-style загрузчик

- BIOS определяет порядок дисков загрузки
- Диск может быть загрузочным
- Первые 512 байт - это MBR
  - если последние байты {0x55, 0xAA}, то диск является загрузочным
  - перед последними двумя байтами хранится таблица первичных разделов (64 байта)
  - первые 446 (512-2-64) байт могут содержать исполняемый код загрузчика

Что может делать загрузчик

- Использовать 1Мб адресного пространства
- Использовать запись в видеопамять (VGA text mode)
- Использовать API, предоставляемый BIOS:
  - доступ к дискам
  - доступ к клавиатуре
  - доступ к COM-порту

Загрузчики

- Примитиивные: ntldr, loadlin
- Поумнее: GRUB
  - имеют загружать разные типы ОС
  - функциональность, достаточная для параметризации загрузки
  - просто симпатичные
  - **в 446 байт такое запихать трудно**

Загрузчик GRUB

- Две стадии загрузки:
  - код из MBR загружает core.img из /boot
  - вторая стадия загружает само ядро

Загрузка ELF-файла

- Адресное пространство переключается в 24-битный реальный режим (Gate A20)
- Загружается ядро **строго после** 1-го мегабайта адресного пространства
- Выполняется поиск Magic Bytes в образе
- Рядом с Magic Bytes - точка входа
- Отключаются программные прерывания
- Ядро переключается в защищенный режим
- Поехали!

Демонстрация кода из toy os

GUID Partition Table

- GUID - Global Unique IDentifier
  128-битный уникальный ключ диска или раздела
- Не имеет значения, к какому из портов подключен диск

GUID Partition Table

- MBR - максимальный размер раздела ~2Tb
- GPT - сотни Tb

- MBR - 4 основных раздела, если нужно больше, то делаются «вложенные» разделы
- GPT - 264 раздела

- Выделяется отдельный раздел EfiBoot (фактически FAT32) для загрузки UEFI

Unified Extensible Firmware Interface

- Программный интерфейс для небольших программ, которые хранятся во Flash-памяти железа:
  - инструменты для тестирования
  - GUI для настроек ПК
  - менеджер загрузки ОС
- Программы UEFI могут храниться как во flash-памяти, так и в EfiBoot разделе по фиксированному URI: EFI\BOOT\BOOTX64.efi
- В Linux EfiBoot обычно монтируется к /boot/efi

Unified Extensible Firmware Interface

- Формат файла - MZ PE
- Используется API функций прошивки, а не прерывания BIOS
  [https://uefi.org/sites/default/files/resources/UEFI_Spec_2_8_final.pdf]
- Выполняется в защищенном режиме процессора