

Операционные Системы

Исполняемые файлы

May 11, 2017

Первый процесс

- ▶ Ядро ОС настроило прерывания, аллокаторы, планировщик. Что дальше?

Первый процесс

- ▶ Ядро ОС настроило прерывания, аллокаторы, планировщик. Что дальше?
 - ▶ мы должны запустить первый процесс и первое приложение!

Первый процесс

- ▶ Ядро ОС настроило прерывания, аллокаторы, планировщик. Что дальше?
 - ▶ мы должны запустить первый процесс и первое приложение!
 - ▶ например, Linux проверяет файлы: /sbin/init, /etc/init, /bin/init и /bin/sh.

Исполняемые файлы

- ▶ Существует множество форматов исполняемых файлов:

Исполняемые файлы

- ▶ Существует множество форматов исполняемых файлов:
 - ▶ ELF, a.out, PE, COM, Mach-O;

Исполняемые файлы

- ▶ Существует множество форматов исполняемых файлов:
 - ▶ ELF, a.out, PE, COM, Mach-O;
 - ▶ скрипты, начинающиеся с `#!` (sha-bang).

Заголовок исполняемого файла

- ▶ Заголовок:

Заголовок исполняемого файла

- ▶ Заголовок:
 - ▶ magic number/string - позволяет быстро определить формат файла;

Заголовок исполняемого файла

- ▶ Заголовок:
 - ▶ magic number/string - позволяет быстро определить формат файла;
 - ▶ различного рода флаги и параметры:

Заголовок исполняемого файла

- ▶ Заголовок:
 - ▶ magic number/string - позволяет быстро определить формат файла;
 - ▶ различного рода флаги и параметры:
 - ▶ версия формата исполняемого файла;

Заголовок исполняемого файла

- ▶ Заголовок:
 - ▶ magic number/string - позволяет быстро определить формат файла;
 - ▶ различного рода флаги и параметры:
 - ▶ версия формата исполняемого файла;
 - ▶ архитектура;

Заголовок исполняемого файла

- ▶ Заголовок:
 - ▶ magic number/string - позволяет быстро определить формат файла;
 - ▶ различного рода флаги и параметры:
 - ▶ версия формата исполняемого файла;
 - ▶ архитектура;
 - ▶ ссылки на другие части файла.

Заголовок ELF файла

```
struct elf64_hdr {  
    uint8_t e_ident[16];  
    uint16_t e_type;  
    uint16_t e_machine;  
    uint32_t e_version;  
    uint64_t e_entry;  
    uint64_t e_phoff;  
    uint64_t e_shoff;  
    uint32_t e_flags;  
    uint16_t e_ehsize;  
    uint16_t e_phentsize;  
    uint16_t e_phnum;  
    uint16_t e_shentsize;  
    uint16_t e_shnum;  
    uint16_t e_shstrndx;  
} __attribute__((packed));
```

Точка входа

- ▶ У любой программы есть первая инструкция - точка входа:

Точка входа

- ▶ У любой программы есть первая инструкция - точка входа:
 - ▶ формат исполняемого файла явно или не явно указывает адрес первой инструкции;

Точка входа

- ▶ У любой программы есть первая инструкция - точка входа:
 - ▶ формат исполняемого файла явно или не явно указывает адрес первой инструкции;
 - ▶ ОС после загрузки исполняемого файла передает управление первой инструкции;

Точка входа

- ▶ У любой программы есть первая инструкция - точка входа:
 - ▶ формат исполняемого файла явно или не явно указывает адрес первой инструкции;
 - ▶ ОС после загрузки исполняемого файла передает управление первой инструкции;
 - ▶ обычно передача управления сопровождается понижением уровня привилегий кода (переходом в userspace).

Заголовок ELF файла

```
struct elf64_hdr {
    uint8_t e_ident[16];
    uint16_t e_type;
    uint16_t e_machine;
    uint32_t e_version;

    /* Logical address of the first instruction */
    uint64_t e_entry;

    uint64_t e_phoff;
    uint64_t e_shoff;
    uint32_t e_flags;
    uint16_t e_ehsize;
    uint16_t e_phentsize;
    uint16_t e_phnum;
    uint16_t e_shentsize;
    uint16_t e_shnum;
    uint16_t e_shstrndx;
} __attribute__((packed));
```

Описание адресного пространства

- ▶ Формат исполняемого файла описывает логическое адресное пространство:

Описание адресного пространства

- ▶ Формат исполняемого файла описывает логическое адресное пространство:
 - ▶ какие участки логического адресного пространства нужны и для чего;

Описание адресного пространства

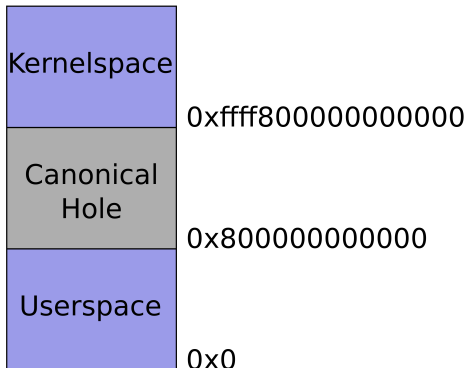
- ▶ Формат исполняемого файла описывает логическое адресное пространство:
 - ▶ какие участки логического адресного пространства нужны и для чего;
 - ▶ где в памяти процесса должны располагаться код и данные;

Описание адресного пространства

- ▶ Формат исполняемого файла описывает логическое адресное пространство:
 - ▶ какие участки логического адресного пространства нужны и для чего;
 - ▶ где в памяти процесса должны располагаться код и данные;
 - ▶ где в исполняемом файле хранятся код и данные.

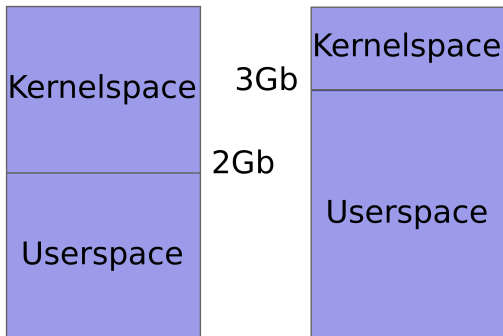
Типичное адресное пространство

x86-64

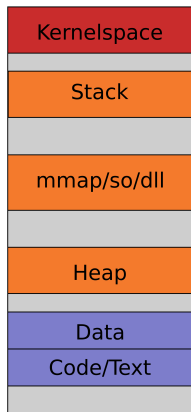


Типичное адресное пространство

x86-32



Типичное адресное пространство



Elf Program Headers

```
struct elf64_hdr {
    uint8_t e_ident[16];
    uint16_t e_type;
    uint16_t e_machine;
    uint32_t e_version;
    uint64_t e_entry;

    /* Offset of the program header table */
    uint64_t e_phoff;

    uint64_t e_shoff;
    uint32_t e_flags;
    uint16_t e_ehsize;

    /* The size of a program header table entry */
    uint16_t e_phentsize;
    /* The number of entries in the program
       header table */
    uint16_t e_phnum;

    uint16_t e_shentsize;
    uint16_t e_shnum;
    uint16_t e_shstrndx;
} __attribute__((packed));
```

Elf Program Headers

```
struct elf64_phdr {  
    /* There are different types of segments,  
       we need PT_LOAD == 1 */  
    uint32_t p_type;  
  
    /* Read/Write/Execute */  
    uint32_t p_flags;  
  
    /* Offset of the segment in the file */  
    uint64_t p_off;  
  
    /* The logical address of the segment in memory */  
    uint64_t p_vaddr;  
    uint64_t p_paddr;  
  
    /* The size of the file image of the segment */  
    uint64_t p_filesz;  
  
    /* The size of the memory image of the segment */  
    uint64_t p_memsz;  
  
    uint64_t p_align;  
} __attribute__((packed));
```

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле
 - ▶ аллоцировать память и настроить таблицы страниц;

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле
 - ▶ аллоцировать память и настроить таблицы страниц;
 - ▶ скопировать код и данные из файла в память;

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле
 - ▶ аллоцировать память и настроить таблицы страниц;
 - ▶ скопировать код и данные из файла в память;
 - ▶ возможно создать стек отдельно.

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле
 - ▶ аллоцировать память и настроить таблицы страниц;
 - ▶ скопировать код и данные из файла в память;
 - ▶ возможно создать стек отдельно.
- ▶ "Прыгнуть" в userspace

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле
 - ▶ аллоцировать память и настроить таблицы страниц;
 - ▶ скопировать код и данные из файла в память;
 - ▶ возможно создать стек отдельно.
- ▶ "Прыгнуть" в userspace
 - ▶ передать управление точке входа, указанной в файле;

Загрузка исполняемого файла

- ▶ Подготовить адресное пространство согласно описанию в файле
 - ▶ аллоцировать память и настроить таблицы страниц;
 - ▶ скопировать код и данные из файла в память;
 - ▶ возможно создать стек отдельно.
- ▶ "Прыгнуть" в userspace
 - ▶ передать управление точке входа, указанной в файле;
 - ▶ возможно, понизить уровень привилегий.

Библиотеки

- ▶ Виды библиотек:

Библиотеки

- ▶ Виды библиотек:
 - ▶ статические - становятся частью исполняемого файла;

Библиотеки

- ▶ Виды библиотек:
 - ▶ статические - становятся частью исполняемого файла;
 - ▶ динамические - хранятся отдельно от исполняемого файла

Библиотеки

- ▶ Виды библиотек:
 - ▶ статические - становятся частью исполняемого файла;
 - ▶ динамические - хранятся отдельно от исполняемого файла
 - ▶ загружаются при запуске приложения или по требованию.

Динамические библиотеки

- ▶ Особенность динамических библиотек - могут быть загружены по разным адресам

Динамические библиотеки

- ▶ Особенность динамических библиотек - могут быть загружены по разным адресам
 - ▶ как код библиотеки обращается к своим коду и данным?

Динамические библиотеки

- ▶ Особенность динамических библиотек - могут быть загружены по разным адресам
 - ▶ как код библиотеки обращается к своим коду и данным?
 - ▶ как код приложения обращается к библиотеке?

Динамические библиотеки

- ▶ Особенность динамических библиотек - могут быть загружены по разным адресам
 - ▶ как код библиотеки обращается к своим коду и данным?
 - ▶ как код приложения обращается к библиотеке?
 - ▶ как код библиотек обращается к коду и данным других библиотек?

Компоновщик

- ▶ Компоновщик (linker, link editor) - программа, которая "связывает" бинарные файлы вместе и генерирует исполняемый файл

Компоновщик

- ▶ Компоновщик (linker, link editor) - программа, которая "связывает" бинарные файлы вместе и генерирует исполняемый файл
 - ▶ в момент компиляции адреса функций/переменных могут быть не известны;

Компоновщик

- ▶ Компоновщик (linker, link editor) - программа, которая "связывает" бинарные файлы вместе и генерирует исполняемый файл
 - ▶ в момент компиляции адреса функций/переменных могут быть не известны;
 - ▶ компилятор просто оставляет "пустое место", а компоновщик записывает в него адрес.

Динамический компоновщик

- ▶ Адреса функций/переменных из динамических библиотек не известны

Динамический компоновщик

- ▶ Адреса функций/переменных из динамических библиотек не известны
 - ▶ компилятор/статический компоновщик оставляют "пустые места";

Динамический компоновщик

- ▶ Адреса функций/переменных из динамических библиотек не известны
 - ▶ компилятор/статический компоновщик оставляют "пустые места";
 - ▶ динамический компоновщик должен записать в них адреса, после того как библиотека была загружена.

Загрузка ELF файла с динамическими библиотеками

- ▶ ELF файл загружается как обычно

Загрузка ELF файла с динамическими библиотеками

- ▶ ELF файл загружается как обычно
 - ▶ ищем Program Header-ы с типом `PT_LOAD` и загружаем их в память.

Загрузка ELF файла с динамическими библиотеками

- ▶ ELF файл загружается как обычно
 - ▶ ищем Program Header-ы с типом `PT_LOAD` и загружаем их в память.
- ▶ Смотрим в Program Header с типом `PT_INTERP`

Загрузка ELF файла с динамическими библиотеками

- ▶ ELF файл загружается как обычно
 - ▶ ищем Program Header-ы с типом `PT_LOAD` и загружаем их в память.
- ▶ Смотрим в Program Header с типом `PT_INTERP`
 - ▶ там хранится имя файла динамического компоновщика;

Загрузка ELF файла с динамическими библиотеками

- ▶ ELF файл загружается как обычно
 - ▶ ищем Program Header-ы с типом `PT_LOAD` и загружаем их в память.
- ▶ Смотрим в Program Header с типом `PT_INTERP`
 - ▶ там хранится имя файла динамического компоновщика;
 - ▶ загружаем его в память в дополнение к программе.

Загрузка ELF файла с динамическими библиотеками

- ▶ ELF файл загружается как обычно
 - ▶ ищем Program Header-ы с типом `PT_LOAD` и загружаем их в память.
- ▶ Смотрим в Program Header с типом `PT_INTERP`
 - ▶ там хранится имя файла динамического компоновщика;
 - ▶ загружаем его в память в дополнение к программе.
- ▶ Передаем управление *динамическому компоновщику*.

Поиск динамических библиотек

- ▶ Исполняемый файл должен хранить информацию о динамических библиотеках

Поиск динамических библиотек

- ▶ Исполняемый файл должен хранить информацию о динамических библиотеках
 - ▶ например, ELF Program Header с типом `PT_DYNAMIC` указывает, где в файле хранится эта информация;

Поиск динамических библиотек

- ▶ Исполняемый файл должен хранить информацию о динамических библиотеках
 - ▶ например, ELF Program Header с типом `PT_DYNAMIC` указывает, где в файле хранится эта информация;
 - ▶ динамический компоновщик загружает все требуемые зависимости в память.

Редактирование связей

- ▶ Исполняемый файл и динамические библиотеки хранят список обращений к внешним сущностям

Редактирование связей

- ▶ Исполняемый файл и динамические библиотеки хранят список обращений к внешним сущностям
 - ▶ вызовы функций из других (и не только) библиотек;

Редактирование связей

- ▶ Исполняемый файл и динамические библиотеки хранят список обращений к внешним сущностям
 - ▶ вызовы функций из других (и не только) библиотек;
 - ▶ обращения к переменным (и не только) из других библиотек;

Редактирование связей

- ▶ Исполняемый файл и динамические библиотеки хранят список обращений к внешним сущностям
 - ▶ вызовы функций из других (и не только) библиотек;
 - ▶ обращения к переменным (и не только) из других библиотек;
 - ▶ динамический компоновщик находит адреса и записывает их в определенные места в памяти.

GOT

- ▶ ELF формат использует Global Offset Table (GOT)

GOT

- ▶ ELF формат использует Global Offset Table (GOT)
 - ▶ код, обращающийся к переменной, знает относительный адрес GOT и номер записи в ней, соответствующей этой переменной;

GOT

- ▶ ELF формат использует Global Offset Table (GOT)
 - ▶ код, обращающийся к переменной, знает относительный адрес GOT и номер записи в ней, соответствующей этой переменной;
 - ▶ компилятор генерирует код, который берет адрес из GOT;

GOT

- ▶ ELF формат использует Global Offset Table (GOT)
 - ▶ код, обращающийся к переменной, знает относительный адрес GOT и номер записи в ней, соответствующей этой переменной;
 - ▶ компилятор генерирует код, который берет адрес из GOT;
 - ▶ динамический компоновщик записывает в GOT правильные адреса при загрузке.

PLT

- ▶ ELF формат также использует Procedure Linkage Table (PLT)

PLT

- ▶ ELF формат также использует Procedure Linkage Table (PLT)
 - ▶ код обращающийся к функции знает относительный адрес PLT и номер "заглушки" в ней, соответствующей этой переменной;

PLT

- ▶ ELF формат также использует Procedure Linkage Table (PLT)
 - ▶ код обращающийся к функции знает относительный адрес PLT и номер "заглушки" в ней, соответствующей этой переменной;
 - ▶ компилятор генерирует код, который вызывает "заглушку" из PLT вместо реальной функции;

PLT

- ▶ ELF формат также использует Procedure Linkage Table (PLT)
 - ▶ код обращающийся к функции знает относительный адрес PLT и номер "заглушки" в ней, соответствующей этой переменной;
 - ▶ компилятор генерирует код, который вызывает "заглушку" из PLT вместо реальной функции;
 - ▶ динамический компоновщик может изменять PLT, а может изменять GOT, к которой "заглушка" из PLT обращается.