Лекция 17
Файловая система

Разграничение доступа

- Разграничение доступа (access control) – одна из основных задач ядер операционных систем
- Процесс (активная сущность) – субъект, запрашивает разрешения на выполнения операций
- Ресурс (пассивная сущность)
- Разграничение доступа дает ответ на вопрос “может или нет”
- Как может – другие механизмы

Разграничение доступа

- Идентификация
- Аутентификация
- Авторизация

Идентификация

- Субъекты систем разграничения доступа должны быть идентифицированы
- На основе идентификатора субъекта принимается решение о предоставлении доступа
- У каждого процесса есть идентификатор (PID), но он плох для работы с персистентными объектами (файловой системой)

Идентификация в POSIX

- Основной субъект - “пользователь” (user)
- Дополнительный субъект - “группа” (group): пользователь имеет одну “основную группу” и может находиться в нескольких “вторичных группах” (в Linux до 32 групп)
- Идентификатор пользователя (uid) – неотрицательное число
- Идентификатор группы (gid) – неотрицательное число

root

- Пользователь с uid == 0 – специальный
- Обычно он называется “root” (это не фиксировано)
- Если процесс запущен пользователем root, для него не действуют ограничения access control, такой процесс может все

Атрибуты пользователя

- Файл с атрибутами пользователей (кроме паролей) - /etc/passwd – но может быть по-другому - PAM
- Файл с парольной информацией - /etc/shadow
- Идентификатор пользователя (uid)
- Идентификатор основной группы (gid)
- Имя пользователя (user name, login)
- Комментарий (например, ФИО человека)
- “Домашний” каталог (home directory)
- Командная оболочка (login shell)

Атрибуты группы

- Идентификатор группы (gid)
- Имя группы (group name)
- Имена пользователей, у которых эта группа является вторичной

Атрибуты процесса

- Реальный идентификатор пользователя (real user id) – (упрощенно) – кто запустил данный процесс, берется от процесса-родителя
- Эффективный и. п. (effective user id - euid) – с какими правами работает данный процесс
- Обычно real user id == effective user id
- Реальный идентификатор группы (real group id - gid)
- Эффективный идентификатор группы (effective group id – egid)
- Процесс может свободно переключаться между своими основной и вторичными группами

Аутентификация

- Аутентификация – проверка подлинности
- Например, поступает команда – от имени какого пользователя она должна быть выполнена?
- Аутентификация – назначение идентификатора пользователя/группы поступающим командам
- Механизмы аутентификации:
  - По паролю
  - По ключу (public/secret key)
  - Биометрия

Аутентификация в Unix

- В результате успешной аутентификации создается процесс корневого интерпретатора командной строки (login shell) с идентификатором аутент. пользователя/группы
- Login shell выполняет скрипты инициализации (например, .login)
- Все процессы для пользователя порождаются (прямо или косвенно) от login shell, и поэтому получают идентификатор пользователя/группы
- Login shell может сам переходить в интерактивный режим, может запускать другие средства взаимодействия с пользователем

Авторизация

- Проверка прав доступа идентифицированного пользователя к заданным ресурсам
- Например, проверка возможности выполнения операции с файловой системой

Атрибуты файла

- Владелец – идентификатор пользователя
- Группа – идентификатор группы
  (у файла только одна группа!)
- Права доступа
- Дополнительные списки прав доступа
  (Access Control List - ACL)

Избирательное управление доступом (discretionary access control)

- Модель владелец-группа-прочие
- Если uid процесса и uid файла совпадают, берется множество прав доступа владельца (user)
- Если один из gid процесса совпадает с gid файла, берется множество прав доступа группы (group)
- Иначе берется множество прав доступа прочих (other)

Множество прав доступа

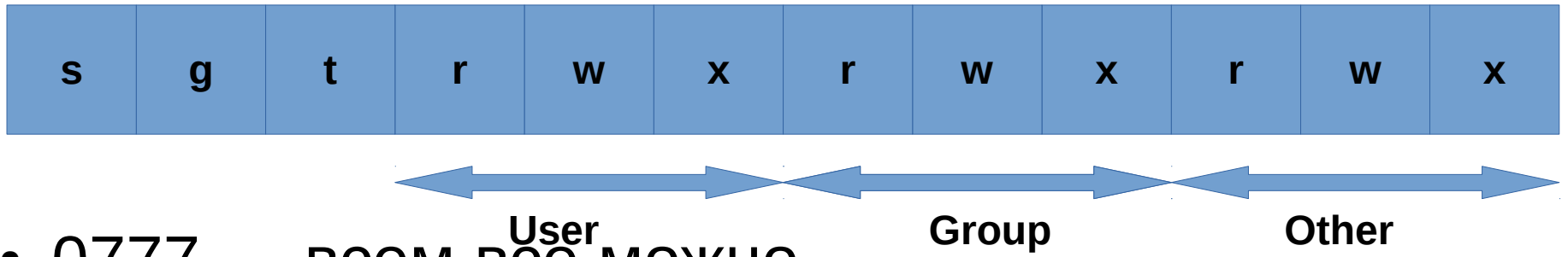
- r,w,x — интерпретация зависит от того, является ли файл каталогом или нет
- Права для файлов:
  - "r" — право на чтение из файла (вызов системного вызова read или lseek)
  - "w" — право на запись в файл (вызов write)
  - "x" — право на выполнение файла (вызов exec*)

Права доступа

- Права для каталогов
  - "r" — право читать список файлов в каталоге (вызовы opendir/readdir/…)
  - "w" — право модифицировать список файлов в каталоге (создавать, удалять, переименовывать)
  - "x" — право на поиск заданного имени в каталоге
- Права "--x" — пользователь не может посмотреть какие файлы есть в каталоге, но если он знает имя файла в нем, с этим файлом может работать

Права доступа

- Полные права — 12 бит (9 основных + 3 доп.)



- 0777 — всем всё можно
- 0664 — чтение/запись для владельца и группы, только чтение для остальных
- 0700 — все права только для владельца

Дополнительные биты

Бит	Для файлов	Для каталогов
S (04000)	При выполнении процесс, запущенный из данного файла, может изменить свой uid на uid файла	Не используется
G (02000)	При выполнении процесс, запущенный из данного файла, может изменить свой gid на gid файла	При создании новых файлов и каталогов группа наследуется из родительского каталога, а не из процесса
T (01000)	Не используется	Только владелец может удалить созданный им файл

Модель файловой системы

- Файловая система размещается на блок-ориентированном устройстве
- Блок-ориентированные устройства:
  - Предоставляют произвольный доступ (seekable)
  - Обмен блоками фиксированного размера
  - Постоянное хранение (повторное чтение одного и того же блока дает один и тот же результат)
- Ядро кеширует блоки устройства в «буферном кеше»

Номер устройства

- Все устройства (блок- и символ-ориентированные) идентифицируются **номером устройства** (st_dev)
- Номер устройства фиксирован в одном сеансе работы, но может меняться после перезагрузки
- Традиционно номер устройства делился на major (24 бита) и minor (8 бит)
  - Major — идентификация типа устройства (напр. SATA диск)
  - Minor — идентификация конкретного устройства

Номер устройства

- Одно блочное устройство — одна файловая система
- Каждая файловая система идентифицируется номером своего блочного устройства
- /dev/loop позволяет отобразить блочное устройство на файл в файловой системе

Блочные устройства