Доклад

Дискреционные модели доступа. Списки управления доступом.

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Легиньких Галина Андреевна
- НФИбд-02-21
- Российский университет дружбы народов
- 1032216447@pfur.ru
- https://github.com/galeginkikh

Введение

Цель работы

Изучить дискреционные модели доступа и списки управления доступом (ACL) как инструментов управления доступом к информационным ресурсам в информационных системах.

Дискреционные модели доступа

Дискреционная модель управления доступом (DAC)

Дискреционная модель управления доступом (Discretionary Access Control, DAC) предоставляет пользователям контроль над правами доступа к их собственным ресурсам. Владельцы файлов и других объектов могут самостоятельно определять, какие пользователи или группы имеют доступ к объекту, и какие действия они могут выполнять.

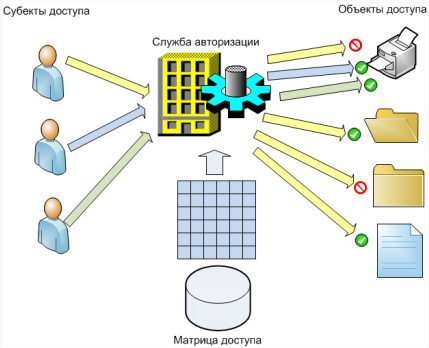

Рис. 1: DAC

Основные принципы DAC

Владение ресурсом: В DAC владелец ресурса имеет полный контроль над тем, кто и каким образом может получать доступ к этому ресурсу.

Гибкость и децентрализация: В отличие от централизованных моделей управления доступом, таких как мандатная модель (MAC), в DAC каждый владелец ресурса управляет доступом к нему самостоятельно.

Преимущества и недостатки DAC

Преимущества

- Гибкость
- Простота управления

Недостатки

- Уязвимость для ошибок
- Отсутствие централизованного контроля

Матрица прав доступа

Матрица прав доступа — это структурированное представление прав доступа, показывающее, какие действия пользователи (субъекты) могут выполнять над ресурсами (объектами). Это важная концепция в модели DAC, которая помогает наглядно представить права доступа в системе.

Структура матрицы прав

Пользователь/Группа	Файл1	Файл2	Директория1
`user1`	r, w	r	r, w, x
`user2`	-	w	r
`group1`	r	-	-

В Linux

В Linux каждая файловая система содержит три базовых типа прав для объектов:

- **Чтение (r)** — возможность просматривать содержимое файла.
- **Запись (w)** — возможность изменять содержимое файла.
- **Исполнение (x)** — возможность запускать файл как программу.

Субъекты управления правами:

- **Владелец (user)** — пользователь, создавший файл или ресурс.
- **Группа (group)** — группа пользователей, которые могут получить доступ к ресурсу.
- **Прочие (other)** — все остальные пользователи.

Списки управления доступом (ACL)

Списки управления доступом (ACL)

Списки управления доступом (Access Control Lists, ACL) представляют собой расширение стандартных прав доступа в Linux, позволяя задавать права для конкретных пользователей и групп, не ограничиваясь базовой триадой (владелец, группа, прочие).

Пример использования ACL в Linux

Установка ACL для файла:

Допустим, у нас есть файл `example.txt`, и мы хотим предоставить пользователю `user1` право на чтение, а пользователю `user2` — право на запись:

```
setfacl -m u:user1:r example.txt
setfacl -m u:user2:w example.txt
```

Пример использования ACL в Linux (Просмотр ACL для файла)

Чтобы увидеть, какие ACL установлены для файла, используйте команду:

```
getfacl example.txt
```

Пример вывода команды:

```
# file: example.txt
# owner: root
# group: root
user::rw-
user:user1:r--
user:user2:-w-
group::r--
mask::rwx
other::r--
```

Удаление ACL:

Если необходимо удалить ACL для конкретного пользователя, используйте команду:

```
setfacl -x u:user1 example.txt
```

Это удалит права доступа, назначенные пользователю `user1`.

Применение DAC и ACL в операционной системе Linux

Команда `chmod` используется для задания прав доступа на файлы и каталоги. Например:

```
chmod 755 example.txt
```

Здесь: - 7 — полный доступ для владельца (чтение, запись, исполнение), - 5 — доступ только на чтение и исполнение для группы и остальных пользователей.

Команда **chown** позволяет изменить владельца файла:

```
chown user1 example.txt
```

Команда **chgrp** изменяет группу, которой принадлежит файл:

```
chgrp group1 example.txt
```

Как посмотреть права доступа в Linux

Пример:

```
ls -l example.txt
```

Результат может выглядеть так:

```
-rw-r--r-- 1 user1 group1 1234 Oct 3 12:34 example.txt
```

Заключение

Заключение

Дискреционная модель управления доступом и списки управления доступом являются важнейшими механизмами контроля прав доступа в операционных системах. Однако правильное использование этих инструментов требует от пользователей и администраторов осторожности и понимания, чтобы избежать ошибок в настройке прав доступа и не допустить утечек информации.