Дискреционные модели доступа. Списки управления доступом.

Доклад

Рогожина Н.А.

19 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Рогожина Надежда Александровна
- Студентка 2го курса, НКАбд-02-22
- Компьютерные и информационные науки
- Российский университет дружбы народов
- Github

Введение

Виды моделей управления доступом

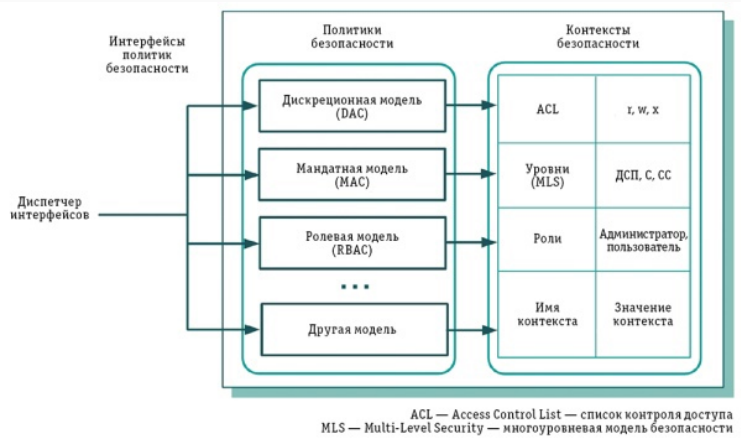

Рис. 1: Виды моделей управления доступом

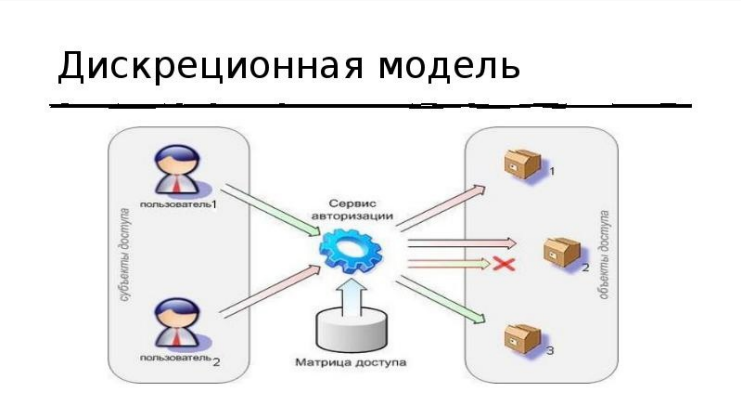

Рис. 2: Схема работы дискреционной модели

Дискреционная модель

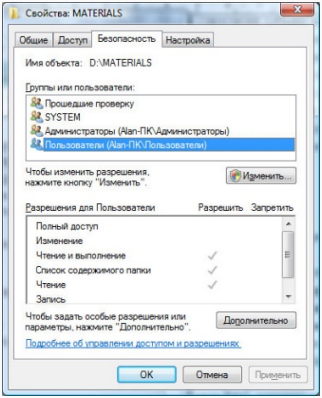

Рис. 3: Пример

Матрица доступа

	Об. А	Об. Б	Об. В	Об. Г	Об. Д
Суб. 1	r w x	r w x	r w x	r w x	r w x
Суб. 2	r w x	r w x	r w x	r w x	r w x
Суб. 3	r w x	r w x	r w x	r w x	r w x
Суб. 4	r w x	r w x	r w x	r w x	r w x
Суб. 5	r w x	r w x	r w x	r w x	r w x

Рис. 4: Матрица доступа

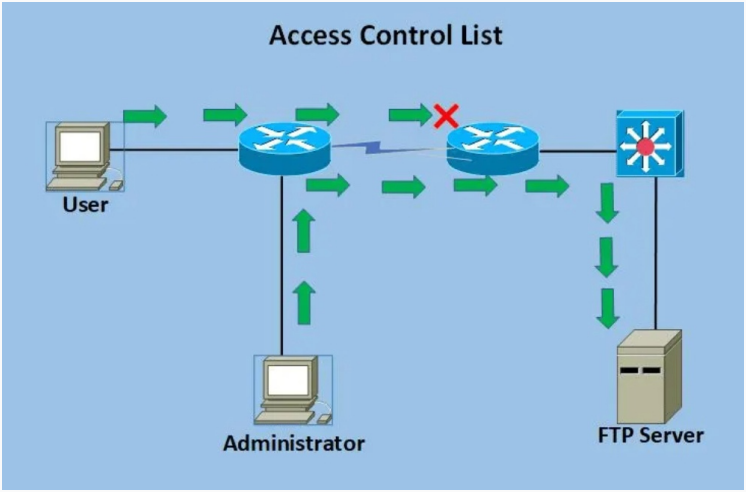

Рис. 5: ACL

Списки контроля доступа (ACL)

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Рис. 6: Пример

Типы ACL

- Стандартные ACL разрешают или запрещают пакеты только на основе IPv4-адреса источника. В них дополнительно используются номера 1300-1999 или 1-99 для определения маршрутизатором точного адреса источника информации. Стандартные ACL не так мощны, как расширенные, но используют меньше вычислительной мощности.
- Расширенные ACL позволяют разграничивать адреса поставки и назначения для определенных узлов или всей сети. С помощью расширенных списков управления доступом можно фильтровать трафик, поддерживаемый протоколами IP, TCP и других (ICMP, UDP).

Типы ACL

- Рефлексивные ACL фильтруют трафик с помощью данных сеанса верхнего уровня. Узел в локальной сети отправляет TCP-запрос в интернет и получает TCP-ответ. Далее формируется дополнительный ACL, распознающий сгенерированные из локальной сети параметры сессий пользователей. Эти параметры служат основой для доступа.
- Динамические ACL надежны в отношении расширенных ACL, Telnet и аутентификации. Они дают администраторам возможность гибко настраивать доступ. Например, предоставить временный доступ пользователю или запретить доступ к маршрутизатору из интернета, но оставить возможность работать с ним группе пользователей.

Выводы

Выводы

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и администратор, имеющий возможность изменения прав для любого объекта и (или) изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем, например, в классических UNIX-системах или в системах Windows семейства NT. Дискреционное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.