Skillbox

Модель управления доступом MAC и DAC

Медведик Давид

Ведущий инженер-программист в «Positive Technologies»

Цель урока

Познакомиться с моделями управления доступом MAC и DAC.

В этом уроке мы рассмотрим

- Модели управления доступом
- Модель дискреционного контроля за доступом(DAC)
- Модель обязательного контроля за доступом(MAC)
- Преимущества и недостатки MAC
- Где применяется MAC

Зачем нам нужно это знать?

- Управление знаниями в интернете
- Понимание связей базы знаний нескольких организаций

Модели управления доступом

Модель управления доступом — это структура, которая определяет порядок доступа субъектов к объектам. Для реализации правил и целей этой модели используются технологии управления доступом и механизмы безопасности.

Модели управления доступом:

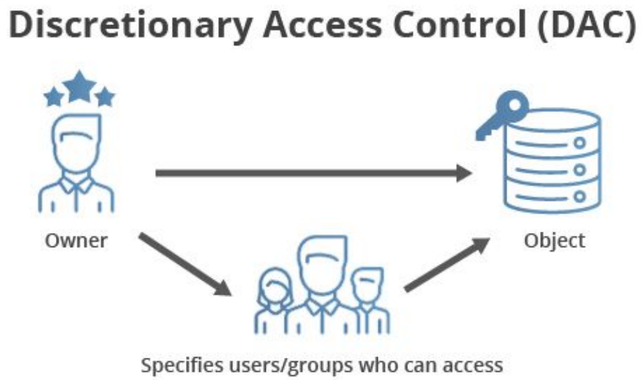
- дискреционная
- мандатная

Управление доступом в распределенной среде:

- централизованное
- децентрализованное

Модель дискреционного контроля за доступом

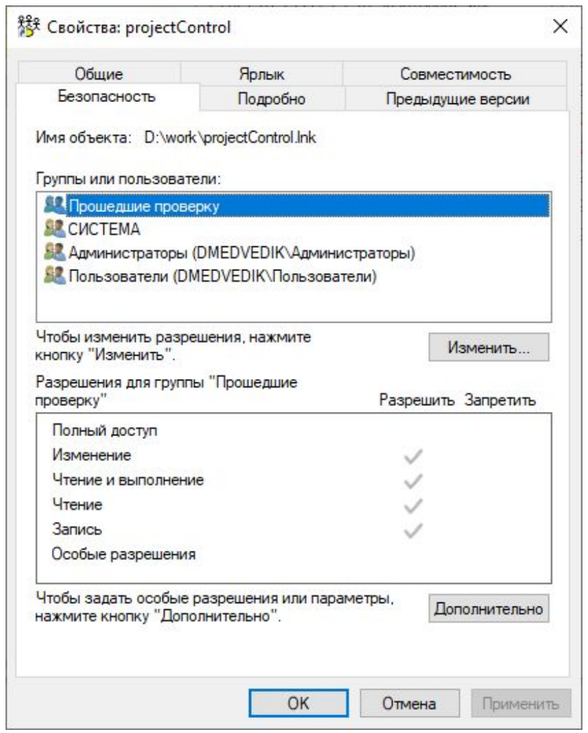
Средства Дискреционного Контроля за Доступом (Discretionary Access Control — DAC) обеспечивают защиту персональных объектов в системе. Контроль является дискреционным в том смысле, что владелец объекта сам определяет тех, кто имеет доступ к объекту, а также вид их доступа.



Модель дискреционного контроля за доступом

Доступ	Доступ субъекта к объекту для определённых операций
Объект	Контейнер информации в системе
Субъект	Сущность, определяющая пользователя при работе в системе
Пользователь	Человек, выполняющий действия в системе, или приложение, выступающее от его имени

Модель дискреционного контроля за доступом

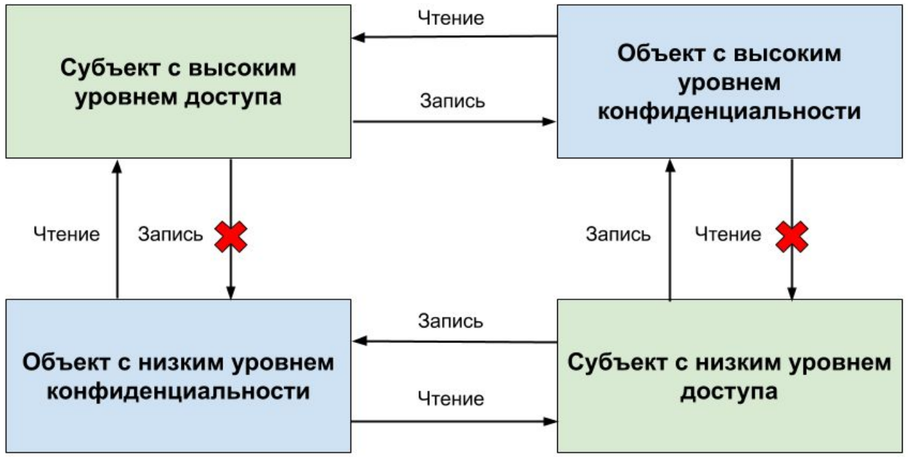


Недостатки DAC

- Не предоставляет полной гарантии, что информация не станет доступна субъектам, не имеющим к ней доступа
- Не устанавливает никаких ограничений на распространение информации
- Все объекты в системе принадлежат субъектам, которые настраивают доступ к ним для других

Модель обязательного контроля за доступом

Средства Обязательного Контроля за Доступом (Mandatory Access Control — MAC). Контроль является обязательным в том смысле, что пользователи не могут изменять стратегию MAC в отношении объектов. При создании объекта система автоматически присваивает ему атрибуты MAC, и изменить эти атрибуты может только администратор, имеющий соответствующие полномочия.



Уровень безопасности

- Совершенно Секретно (СС)
- Секретно (С)
- Конфиденциально (К)
- Рассекречено (Р)

При этом верно следующее: СС > С > К > Р

Преимущества и недостатки MAC

Плюсы:

- высокая степень надёжности, практически исключён взлом
- автоматизированная проверка и обеспечение прав доступа
- данные не могут быть изменены несанкционированно

Минусы:

- требует много планирования
- система MAC достаточно громоздкая, администраторы сильно загружены
- долгий и дорогостоящий процесс перехода на MAC

Где применяется MAC?

- В операционной системе SELinux на основе архитектуры Flux Advanced Security Kernel (FLASK)
- FreeBSD Unix, SUSELinux, Ubuntu Linux (AppArmor)
- В отечественных операционных системах Astra Linux Special Edition
- PostgreSQL Pro

Вывод

Теперь у вас более чёткое представление о том, как устроены модели управления доступом, и как они используются.