УПРАВЛЕНИЕ ДОСТУПОМ

Лекция 13

Дискреционное управление доступом

Матрица прав доступа

Файлы Пользователи	F1	F2	F3	F4	F5
Петров		R			
Иванов		RW	R		
Федоров					RW
Сидоров	C	C	C	C	C

Строки соответствуют субъектам – активной составляющей (пользователи, процессы и т. д.).
Столбцы соответствуют объектам – пассивной составляющей (файлы, каталоги, процессы и т.д.).
Ячейки – права доступа (R права доступа по чтению, W – права доступа по записи, C – право на
создание объекта.

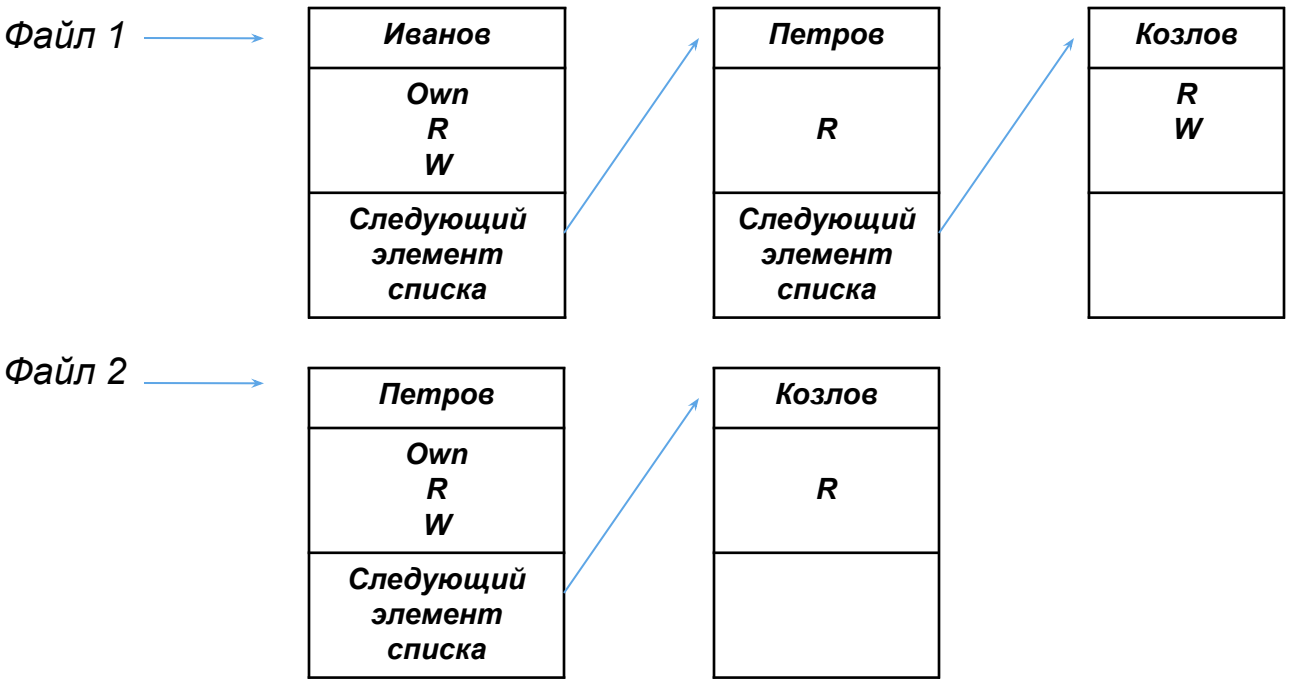
Дискреционное управление доступом

Механизмы реализации матрицы прав доступа в ОС.

- Списки прав доступа ACL (Access Control List)
- Биты защиты

Дискреционное управление доступом

Пример списка прав доступа



Преимущество – возможность задания прав доступа индивидуально для каждого пользователя.

Недостаток – большие временные затраты на обработку списков по сравнению с доступом с помощью битов защиты.

Контроль доступа в Windows NT

Поддерживается произвольное управление доступом (*discretionary access control, DAC)* с помощью ACL. Каждый объект имеет свой ACL, который состоит из так называемых сущностей контроля доступа (Access Control Entries – ACE). Существует 3 типа ACE: ACE Allowed (разрешает указанный тип доступа), ACE Denied (запрещает), третий используется для аудита. Первые 2 ACE содержат маску доступа, определяющую разреш. или запрещ. типы доступа.

Алгоритм контроля доступа в Windows NT

1. Система сравнивает идентификатор процесса, запросившего доступ с идентификаторами, присутствующими в ACL объекта. Если в ACL отсутствует упоминание этого идентф. то доступ запрещается. Если идентиф. присутствует в ACL, то сначала обрабатывается ACE типа Denied, а затем типа Allowed.
2. Для всех ACE, имеющих тип Denied, запрашиваемый тип доступа сравнивается с

Алгоритм контроля доступа в Windows NT

указанным в маске ACE. Если хотя бы один тип доступа (чтение, запись и т.д.) присутствует в обеих масках, то доступ запрещается. После обработки всех ACE этого типа начинается обработка элементов типа Allowed.

3. Для всех ACE типа Allowed запрашиваемый тип доступа сравнивается с указанным в маске ACE. Если все типы доступа в запросе встретились в масках ACE, доступ разрешается, если не все – запрещается.

Дискреционное управление доступом

Биты защиты ОС UNIX

Владелец			Группа			Все пользователи		
Чтение	Запись	Выполн.	Чтение	Запись	Выполн.	Чтение	Запись	Выполн.
1	2	3	4	5	6	7	8	9

Алгоритм предоставления прав доступа.

Субъект ассоциируется с эффективным идентификатором (EUID), содержащим информацию о пользователе и группе, к которой он принадлежит.

1. Проверяется, является ли субъект владельцем. При этом сравниваются значения EUID процесса и EUID' владельца объекта. Если EUID'= EUID, то сравниваются полномочия владельца с запрашиваемым типом доступа. Если запрашиваемый тип доступа присутствует в соответствующем поле, доступ предоставляется. Если нет, отклоняется. Если идентификаторы не равны, то осуществляется переход ко второму шагу.

Дискреционное (произвольное) управление доступом

Алгоритм предоставления прав доступа в ОС UNIX (продолжение).

- **2.** Проверка соответствия полномочий входящего в группу владельца осуществляется аналогично п.1.
- **3.** Сравниваются полномочия, предоставленные всем пользователям системы с запрашиваемым типом доступа. Если запрашиваемый тип присутствует в соответствующем поле, то доступ предоставляется, если нет – отклоняется.

Мандатное (нормативное, принудительное) управление доступом (1)

Мандатное управление доступом (*Mandatory access control, MAC*) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как **Принудительный контроль доступа**.

Мандатное (нормативное, принудительное) управление доступом (2)

Способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования. Например, субъект «Пользователь № 2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющего метку «для служебного пользования». В то же время, субъект "Пользователь «№ 1» с допуском уровня «секретно», право доступа к объекту с меткой «для служебного пользования» имеет.

Модель Белла — Лападулы (1)

Модель Белла — Лападулы является моделью разграничения доступа к защищаемой информации. Она описывается конечным автоматом с допустимым набором состояний, в которых может находиться информационная система. Все элементы, входящие в состав информационной системы, разделены на две категории — субъекты и объекты. Каждому субъекту присваивается свой уровень доступа, соответств. степени конфиденциальности. Аналогично, объекту присваивается уровень секретности.

Модель Белла — Лападулы (2)

Понятие защищённой системы определяется следующим образом: каждое состояние системы должно соответствовать политике безопасности, установленной для информационной системы. Переход между состояниями описывается функциями перехода. Система находится в безопасном состоянии в том случае, если у каждого субъекта имеется доступ только к тем объектам, к которым разрешен доступ на основе текущей политики безопасности. Для определения, имеет ли субъект права на получение определенного вида доступа к объекту, уровень секретности субъекта сравнивается с уровнем секретности объекта, и на основе этого сравнения решается вопрос, предоставить или нет запрашиваемый доступ.

Нормативное управление доступом

Модель Белла-Лападулы

1.Простое свойство безопасности (запрет чтения с верхнего уровня).

Субъект с уровнем безопасности X может читать информацию из объекта с уровнем безопасности Y, только если X преобладает над Y.

2.Свойство -* (star property) (запрет записи на нижний уровень).

Субъект с уровнем безопасности X может писать информацию в объект с уровнем безопасности Y, только если Y преобладает над X.

Модель Белла — Лападулы

Диаграмма информационных потоков

Научная база

«Безопасный Linux» Security-Enhanced Linux — наиболее известная и мощная система обеспечения мандатного контроля доступа в операционных системах GNU/Linux.

Trusted Information Systems (**TIS**) was a computer security research and development company during the 1980s and 1990s, performing computer security research for organizations such as NSA, DARPA, ARL, AFRL, SPAWAR, and others.

Научная база

Mach is an operating system kernel developed at Carnegie Mellon University to support operating system research, primarily distributed and parallel computation. It is one of the earliest examples of a microkernel. Its derivatives are the basis of the modern operating system kernels in Mac OS X and GNU Hurd.

TIS projects included Trusted Xenix, the first commercially available B2 operating system; Trusted Mach, a research project that influenced DTOS and eventually SELinux;

SELinux

Исследовательский проект АНБ SELinux добавил архитектуру мандатного контроля доступа к ядру Linux, и позднее был внесён в главную ветвь разработки. **SELinux** (*Security-Enhanced Linux* — Linux с улучшенной безопасностью) — реализация системы мандатного управления доступом, которая может работать параллельно с классической дискреционной системой управления доступом. Входит в стандартное ядро Linux.

Дискреционное управление доступом Trusted Mach

Пример типов прав системы Trusted Mach

- **Право на чтение** подразумевает возможность просматривать, но не модифицировать информацию, содержащуюся в объекте;
- **Право на запись** означает возможность просматривать и модифицировать содержимое объекта;
- **Право на добавление** подразумевает возможность модифицировать содержимое объекта, но без возможности чтения (т.н. «слепая запись»);
- **Право создания** объекта означает возможность создавать объект;
- **Право управления доступом** подразумевает возможность уничтожать объект и изменять права доступа к нему в соответствии с политикой произвольного управления доступом.

Общая модель управления доступом на примере Trusted Mach

Правила политики безопасности

1. Для того чтобы субъект получил к объекту доступ по чтению, уровень безопасности субъекта должен доминировать над уровнем безопасности объекта. Кроме того, субъект должен иметь дискреционные полномочия на чтение этого объекта.

2. Для того чтобы субъект получил доступ записи к объекту, уровень безопасности субъекта должен совпадать с уровнем безопасности объекта. Кроме того, субъект должен иметь дискреционные полномочия на запись в этот объект.

3. Для того чтобы субъект получил возможность добавить данные в объект, уровень безопасности объекта должен доминировать над уровнем безопасности субъекта. Кроме того, субъект должен иметь дискреционные полномочия на добавления данных в этот объект.

4. Для того чтобы субъект мог осуществлять управление доступом к объекту, субъект и каталог, в котором содержится этот объект, должны иметь один и тот же уровень безопасности. Кроме того, политика произвольного управления доступом должна разрешать субъекту управление доступом для этого объекта.

5. Субъект может создавать объекты, уровень безопасности которых доминирует над его уровнем безопасности. Кроме того, субъект должен иметь дискреционные полномочия на создание объектов этого типа.

Нормативное управление доступом является определяющим

Дискреционное управление доступом в системе Trusted Mach

ACL системы Trusted Mach

Формат элементов списка

- *<тег>:<идентификатор>:<разрешенные права>:<запрещенные права>*
- *Тег* – одно из ключевых слов “user”, “group”, “all”;
- *Идентификатор* – в зависимости от значения поля *тег*, либо идентификатор пользователя (в поле *тег* указано *user*), либо идентификатор группы (в поле *тег* стоит “group”), либо символ шаблона «*» (поле *тег* содержит all);
- *Разрешенные права доступа* – список разрешенных прав доступа (none означает пустой список);
- *Запрещенные права доступа* – список запрещенных прав доступа (none означает пустой список).
- **Например:**
- user : john : read, write : none
- group : programmers : read, write : none
- group : users : none : read
- all:* : read : none

Дискреционное управление доступом в системе Trusted Mach

Условия, необходимые для разрешения конфликтов

- 1. Запрашиваемые права доступа должны отсутствовать во всех элементах списка запрещенных прав доступа, применимых к данному субъекту.

- 2. Запрашиваемые права доступа должны присутствовать хотя бы в одном элементе списка разрешенных прав доступа, который относится к данному субъекту.

Дискреционное управление доступом в системе Trusted Mach

Алгоритм обработки списка прав доступа

1. Сначала в списке прав доступа ищутся элементы, для которых в поле <*идентификатор*> указано имя субъекта, запросившего доступ к объекту. Программа контроля доступа просматривает все записи подобного вида и комбинирует из них индивидуальные наборы разрешенных и запрещенных прав доступа. Если хотя бы **одно** из запрашиваемых прав доступа присутствует в списке запрещенных, то в доступе отказывается. Если **все** без исключения запрашиваемые права доступа входят в набор разрешенных прав, то доступ разрешается. Если **ни одно** из запрашиваемых прав не присутствует в наборе запрещенных, но **не все** запрашиваемые права указаны в наборе разрешенных, то вступает в силу управление доступом на уровне групп.

2. Управление доступом на уровне групп выполняется аналогично 1. К групповому набору разрешенных прав добавляется индивидуальный набор, полученный на предыдущем этапе.

3. Управление доступом на уровне шаблонов выполняется аналогично 1, 2. К шаблону разрешенных прав добавляются индивидуальный и групповой наборы разрешенных прав, полученные на предыдущих этап.

Управление доступом в МСВС 3.0

Основные понятия

- Сопоставляются классификационные метки (метки безопасности) каждого субъекта и каждого объекта.
- Метка субъекта описывает его благонадежность, метка объекта — степень закрытости содержащейся в нем информации.
- Метки безопасности состоят из двух частей — уровня секретности и списка категорий.
- Уровни секретности образуют упорядоченное множество, которое может выглядеть, например, так: особо важно; совершенно секретно; секретно; конфиденциально; несекретно.
- Категории образуют неупорядоченный набор. Их назначение — описать предметную область, к которой относятся данные. В военном окружении каждая категория может соответствовать, например, определенному виду вооружений. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности.

Управление доступом в МСВС 3.0

Правила управления

- Управление доступом основано на сопоставлении меток безопасности субъекта и объекта.
- Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен — читать можно только то, что положено.
- Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может — в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Управление доступом в МСВС 3.0

Поддержка СВТ

- В СВТ реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД.
- Поддерживается до 8 уровней секретности (от 0 — самый несекретный до 7 — самый секретный) и до 61 различных категорий.

Управление доступом в МСВС 3.0

Мандатные метки

- Мандатные метки называются равными, если равны их уровни и равны наборы (векторы) категорий.
- Мандатная метка М1 называется более высокой, чем мандатная метка М2, если а) ее уровень выше (а векторы категорий равны), или б) ее вектор категорий включает в себя вектор категорий метки М2 (а уровни равны), или в) уровень М1 более высокий, чем уровень М2 и вектор категорий М1 включает в себя вектор категорий М2. (Соответственно мандатная метка М2 называется по отношению к М1 более низкой).
- Мандатные метки называются несравнимыми, если их векторы категорий не включают друг друга.

Примеры

- M1 {0x0, 0x1}, где 0x0 это уровень, а 0x1 это вектор категорий (в данном случае состоящий из одного бита) является более низкой, чем M2 {0x2, OxFF}, поскольку уровень M1 (0x0) ниже чем уровень M2 (0x2) и вектор категорий M1 (0x1) включается в вектор категорий M2 (OxFF).
- M3 {0x2, Ox10D2FF} является более высокой чем M2.
- M4 {0x2, Ox30D2FF} является более высокой чем M3.
- M5 {0x2, Ox20D2FF} является более низкой, чем M4 и несравнимой с M3.
- Мб {0x3, Ox20D2FF} является более высокой, чем M5 и несравнима с M3.

Управление доступом в МСВС 3.0

Доступ процессов к файловой системе

- Согласно мандатной политике доступ процессов к файловой системе определяется следующим образом:
- - если мандатные метки процесса и файла (каталога) совпадают (равны), то доступ разрешается полностью — так, как если бы мандатных ограничений не было;
- - если мандатная метка процесса выше, чем мандатная метка файла (каталога), то доступ разрешается только на чтение и исполнение;
- - если мандатная метка процесса ниже мандатной метки файла (каталога), то доступ разрешается только на запись;
- - если мандатные метки процесса и файла несравнимы, то доступ запрещается полностью.

Управление доступом в МСВС 3.0

Определение доступа в соответствии с мандатной моделью полностью независимо от дискреционной модели. Процесс получит доступ к файлу только, если он ему разрешен и согласно мандатной политике и согласно дискреционной политике. Если мандатные или дискреционные ограничения не разрешают доступ процесса к файлу, то он его не получит.

Управление доступом в Trusted Xenix

В системе Trusted Xenix произвольное управление доступом обеспечивается битами защиты и ACL. В начале осуществляется проверка битов защиты владельца и группы. После этого, если существует ACL, то сначала проверка на наличие записей , в которых участвует идентификатор пользователя и его группы. Затем проверяются биты защиты для всех остальных. Нормативное управление доступом опирается на иерархич. группы и неиерархические категории. Поддерживается 255 уровней и 64 катег. Доступ предоставляется только в том случае, если он одновременно разрешен механизмами произвольного и нормативного контроля доступа.