СОДЕРЖАНИЕ

Введение

В последнее время наряду с традиционными моделями дискреционного и мандатного доступа серьезное внимание уделяется моделям доступа, построенным на основе ролей. Особенно активно данная модель изучается в контексте решения задач защиты информации в автоматизированных системах. Это связано с тем, что в основу модели положена идея принадлежности всех данных системы некоторой организации, а не пользователю, как в случае моделей дискреционного и мандатного доступа. В целом модель ориентирована на упрощение и обеспечение формальной ясности в технологии обеспечения политики безопасности системы. Разрешения на использование конкретных данных выдается пользователю администратором в соответствии с ролью, которая ему предписывается при выполнении конкретной функции некоторого технологического процесса. Управление доступом к данным самим пользователем (в том числе и с помощью передачи привилегий) не предусмотрено.

Администрирование ролевой моделью доступа является многоаспектным. Необходима разработка корректного механизма создания и управления в рамках данной модели иерархии административных ролей, обеспечивающих управление процессом доступа к данным. Представленная ролевая модель включает три компонента: модель отображения пользователь – роль, модель отображения привилегия – роль и модель отображения роль – роль.

Для упрощения логической структуры объектов управления вводится понятие иерархии ролей. Роль, входящая в иерархию, может включать другие роли, наследуя все привилегии включаемых ролей.

Для реализации политики безопасности организации на основе базовой модели вводится механизм ограничений. Ограничения позволяют поддерживать роли, для которых политика безопасности не допускает одновременное их отображение на конкретного пользователя, так

называемые взаимно исключающие роли. Другие распространенные варианты ограничения: кардинальное число роли и роли с необходимым предусловием.

Модель отображения пользователь – роль ориентирована на обеспечение корректного отображения множества пользователей на множество ролей в условиях децентрализованного управления. Предлагаемое решение основывается на поддержке специальных отношений “разрешено_назначить” и “разрешено_отозвать”. Аналогичный подход предлагается для реализации модели отображения привилегия – роль. Для модели отображения роль – роль предусматривается реализация трех классов ролей: возможности (abilities), группы и универсальные роли (UP-roles).

Ролевая модель доступа получила определенное распространение в мировой практике обеспечения защищенных технологий обработки данных. Понятие роли, представленное в коммерческой реализации СУБД Oracle, позднее вошло составной частью в стандарт SQL3 и стандарт Common Criteria для коммерческого профиля безопасности.

I. КОНТРОЛЬ И РАЗГРАНИЧЕНИЕ ДОСТУПА

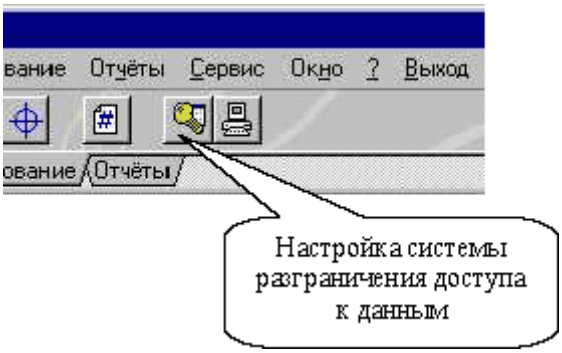
1.1. Понятие разграничение доступа

Вполне естественно, что с системой работает множество пользователей: операторы, диспетчеры, администраторы, бухгалтеры и т.п. Возникает необходимость разграничить права доступа различных категорий пользователей к данным, чтобы исключить возможность искажения хранимой информации и ограничить доступ к ней посторонних.

В силу архитектуры системы, доступ к данным контролируется на двух уровнях: Первый на уровне сервера базы данных (подключение и организация доступа средствами сервера: GRANT SELECT, INSERT, UPDATE, DELETE, EXECUTE, REFERENCES к объектам базы данных), Второй - на уровне функциональности системы ("Разрешить изменять информацию о поступлении средств на дисконтные карты только для группы "Бухгалтеры"" и т.п.). На уровне сервера модель безопасности звучит как "запрещено всё, что не разрешено". На уровне функциональности - "разрешено всё, что не запрещено". Реализованная система безопасности обеспечивает эффективное разграничение прав пользователей в рамках поставленной задачи.

Система безопасности

Меню "Администрирование" - "Разграничение доступа" в Инструментальной панели.



Пользователи и группы

Согласно модели, реализованной в системе, к объектам базы данных могут иметь доступ пользователи, предварительно зарегистрированные

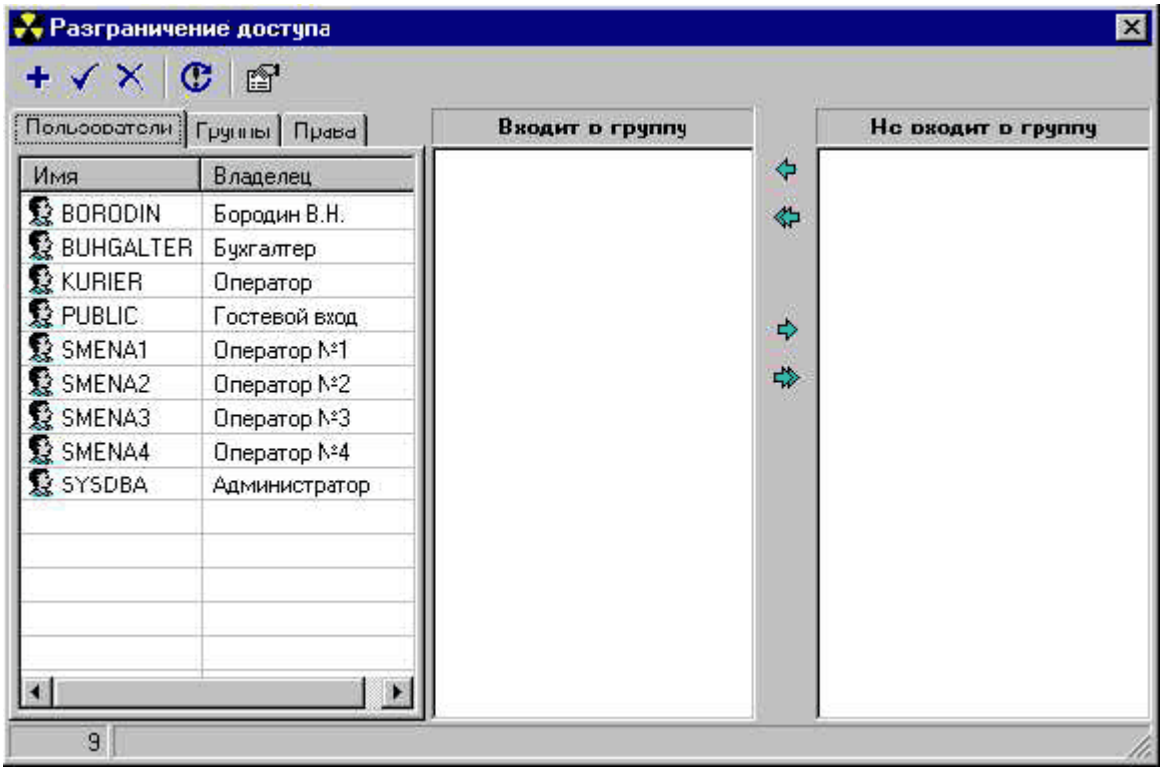
администратором базы данных на сервере. Пользователи объединяются в группы для облегчения администрирования. Права доступа могут быть предоставлены группе. Пользователь может входить в любое количество групп. Группы не могут входить в состав других групп. Права пользователя определяются как сумма прав всех групп, в состав которых он входит.

Права доступа

Под "правом доступа" в системе подразумевается возможность выполнения некоторого действия, требующая явного указания пользователя, имеющего разрешение его совершить.

Например возможность удаления данных за указанный период имеет смысл предоставить не всем пользователям, а только Администраторам системы для предотвращения случайного выполнения команды недостаточно квалифицированным пользователем. Для реализации подобного ограничения вводиться право "Удаление данных за период" и оно предоставляется группе "Администраторы" в которую включаются пользователи, имеющие подобные разрешения. При попытке пользователя получить доступ к этой функции, система проверит наличие соответствующих разрешений и разрешит или запретит выполнение команды.

Настройка системы безопасности



Пользуйтесь методом Drag&Drop.

Система безопасности на уровне функциональности программы может быть отключена, в этом случае вся функциональность будет доступна любому пользователю. Система безопасности на уровне сервера отключена быть не может.

1.2. Создание политики безопасности

Процесс описания правил разграничения доступа в такой хорошо спроектированной системе, как Check Point FireWall-1, прост и очевиден. Все аспекты политики информационной безопасности организации могут быть специфицированы с использованием графического интерфейса FireWall-1, который неоднократно завоевывал различные награды. При определении элементов сети применяется объектно-ориентированный подход.

Будучи создан, объект затем используется для определения политики безопасности при помощи редактора правил. Каждое правило может оперировать любой комбинацией сетевых объектов, сетевых сервисов, а также содержит в себе определение предпринимаемых действий и способов уведомления о срабатывании данного правила. Дополнительно можно

указать, на какие узлы безопасности данное правило должно распространяться. По умолчанию правила действуют на всех шлюзах с установленным FireWall-1. Поддерживаются различные платформы, включая UNIX и NT, а также различное межсетевое оборудование OPSEC партнеров компании Check Point.

Уникальное преимущество Check Point FireWall-1 - это возможность создать единую политику безопасности для всего предприятия в целом. После создания политики безопасности FireWall-1 проверяет ее на непротиворечивость, компилирует и распределяет по всем узлам контроля трафика в сети.

1.3. Распределенный доступ

Архитектура FireWall-1 позволяет беспрепятственно наращивать возможности продукта по мере возрастания потребностей организации во внедрении различных элементов информационной безопасности. С другой стороны, административные функции FireWall-1 также ориентированы на многопользовательский доступ и предоставляют организации возможность разграничить функции администраторов системы безопасности. После авторизации администратор системы FireWall-1 наследует те права, которые установил администратор безопасности для этого FireWall-1 и которые

специфицируются редактором правил. Это дает возможность администрировать несколько систем FireWall-1 с одного рабочего места одновременно.

FireWall-1 поддерживает различные уровни административного доступа:

- **Read/Write:** полный доступ ко всем функциональным возможностям административных средств
- **User Edit:** дает возможность изменять учетные записи пользователей, остальные возможности ограничены правами на чтение
- **Read Only:** доступ только на чтение
- **Monitor Only:** доступ на чтение к средствам визуализации статистики

1.4. Элементы защиты от несанкционированного доступа

IP Spoofing - способ воздействия на элементы сетевой инфраструктуры или получения не авторизованного доступа. В этом случае взломщик подменяет IP адреса в пакетах с целью сделать их похожими на пакеты от более привилегированного источника. Для примера, пакеты, порожденные в Интернет, могут выглядеть как локальные пакеты. FireWall-1 защищает от подобного рода воздействий, легко распознает такие попытки и сообщает о них оператору.

Denial of Service Attack - использует слабости TCP протокола. В момент инициализации TCP-соединения клиент посылает пакет - запрос серверу с установленным флагом SYN в заголовке TCP. В нормальном случае сервер отвечает SYN/ACK-подтверждением, адресованным клиенту, адрес которого сервер берет из IP заголовка полученного запроса. Получив такое подтверждение, клиент посылает уведомление о начале передачи данных – пакет, в TCP заголовке которого установлен флаг ACK. Если адрес клиента подменен (spoofed), например, на несуществующий в Интернет, то такой вариант установления связи не может быть завершен, и попытки будут

продолжаться, пока не исчерпается лимит по времени. Эти условия составляют основу данного вида атак.

Решения, основанные на применении программ-посредников, сами по себе не в состоянии защитить от атак SYN flooding. Таким образом, шлюз может быть атакован для создания условий отказа в обслуживании. Пакетные фильтры тоже не в состоянии защитить от подобного рода атак, так как они не имеют необходимой информации о состоянии соединений и не могут проводить инспекцию пакетов с учетом этого состояния. FireWall-1 предлагает встроенную защиту от подобных атак, располагая всеми необходимыми средствами для анализа состояния соединений и используя механизм SYNDefender.

Ping of Death - практически каждая операционная система, а также некоторые маршрутизаторы, имеют различные ограничения, связанные с конкретной реализацией TCP/IP протокола. Выявление этих ограничений часто связано с появлением новых видов атак. Так, большинство ОС чувствительны к PING (ICMP), размер поля данных которых больше, чем 65508. В результате, ICMP-пакеты после добавления необходимых заголовков становятся больше чем 64k (длинна заголовка составляет 28 байт) и, как правило, не могут правильно обрабатываться ядром операционной системы, что проявляется в виде случайных крушений или перезагрузок.

FireWall-1, обладая механизмом Stateful Inspection, может осуществлять защиту от таких атак, для чего необходимо определить объект типа протокол и добавить правило, которое запрещает прохождение ICMP пакетов, длиннее 64K.

<="" a="" style="color: rgb(0, 0, 0); font-family: 'Times New Roman'; font-size: medium; font-style: normal; font-variant: normal; font-weight: normal; letter-spacing: normal; line-height: normal; orphans: auto; text-align: justify; text-indent: 0px; text-transform: none; white-space: normal; widows: auto; word-spacing: 0px; -webkit-text-size-adjust: auto; -webkit-text-stroke-width: 0px; background-color: rgb(255, 255, 255);">

Примеры методов защиты

Сокрытие Firewall - в нормальных условиях любой пользователь корпоративной сети потенциально может получить доступ к шлюзу с firewall. Этой ситуации необходимо избегать, для чего нужно предпринять меры для сокрытия шлюзового устройства.

Check Point FireWall-1 позволяет реализовать это путем добавления одного простого правила в политику безопасности. Сокрытие шлюза, таким образом, предотвращает любые попытки взаимодействия любого пользователя или приложения со шлюзом безопасности, и делает такой шлюз невидимым. Исключение составляют только администраторы системы безопасности.

Применение механизмов **Трансляции Сетевых Адресов** позволяет полностью скрыть или замаскировать внутреннюю сетевую структуру.

<="" a="">Расширенные возможности сбора статистики и генерация предупреждений

Connection Accounting - FireWall-1, помимо обычной регистрации факта соединения, предоставляет возможность получить интегральные данные о продолжительности, количестве переданных байтов информации и количестве переданных пакетов в данной сессии.

Эти данные записываются в регистрационный журнал в тот момент, когда отслеживаемая сессия заканчивается. Дополнительно можно проследить за параметрами активных соединений.

Active Connections - в FireWall-1 администратор системы безопасности может, используя то же средство просмотра и анализа статистики - Log Viewer - отслеживать активные соединения через модули брандмауэров. Эта статистика в реальном времени обрабатывается и предоставляется оператору так же, как и обычные записи. Они заносятся в специальный файл и находятся там до тех пор, пока соединение не будет закрыто. Это позволяет использовать те же механизмы отбора событий, как и при работе с обычным файлом статистики. Заметим, что при использовании опции сбора

дополнительной информации о соединениях данные интегральной статистики непрерывно обновляются, так, что администратор безопасности может отслеживать не только сам факт соединения, но и интенсивность информационного обмена по нему в реальном времени.

Различные возможности уведомления - FireWall-1 включает в себя множество различных опций для уведомления операторов: от уведомления по электронной почте до возможности посылки SNMP-исключений (traps) для интеграции с такими платформами сетевого управления как HP OpenView, SunNet Manager, IBM's NetView 6000. В дополнение к основным механизмам уведомлений предусмотрена возможность создавать собственные варианты обработки ситуаций, требующих уведомления. Это предоставляет возможность стыковки системы защиты с пэйджинговыми службами или системами быстрого реагирования.

II. АНАЛИЗ СРЕДСТВ РАЗГРАНИЧЕНИЯ ДОСТУПА К ОБЪЕКТАМ В ОПЕРАЦИОННЫХ СИСТЕМАХ MICROSOFT WINDOWS И LINUX

2.1. Модели разграничения доступа

Основу политики безопасности для компьютерной системы любой организации составляют правила разграничения доступа к объектам компьютерной системы. Разграничение доступа к компьютерным ресурсам базируется на различных моделях управления доступом. В данном докладе будут представлены результаты сравнительного анализа средств разграничения доступа к объектам операционных систем Microsoft Windows и Linux.

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретного субъекта. Правом редактирования дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности. Эта модель отличается простотой реализации, но возможна утечка конфиденциальной информации даже в результате санкционированных действий пользователей.

Мандатная модель разграничения доступа предполагает назначение объекту метки (грифа) секретности, а субъекту – уровня допуска. Доступ субъектов к объектам в мандатной модели определяется на основании правил «не читать выше» и «не записывать ниже». Использование мандатной модели, в отличие от дискреционного управления доступом, предотвращает утечку конфиденциальной информации, но снижает производительность компьютерной системы.

Ролевая модель разграничения доступа основана на конструировании ролей и назначении их пользователям на основании выполняемых ими конкретных должностных обязанностей. При назначении и использовании ролей возможно наложение динамических и статических ограничений на совмещение разных ролей одним субъектом, одновременное использование

одной роли разными субъектами и т.п. Подобный подход к разграничению доступа к объектам позволяет разделить обязанности между конструктором ролей и диспетчером ролей, а также более точно связать права доступа пользователей к объектам компьютерной системы с их обязанностями в организации, исключить избыточность полномочий.

В операционных системах Microsoft Windows и операционных системах клона Unix обычно применяется дискреционное управление доступом к объектам. Объекты разграничения доступа в Windows имеют дескриптор безопасности, содержащий информацию о владельце объекта (его идентификаторе безопасностиSID, Security Identifier) и дискреционном списке управления доступом к объекту (Discretionary Access Control List, DACL), правом редактирования которого обладают владелец объекта и администратор. Владелец файла может лишить администратора права изменения разрешений на доступ к объекту. Администратор обладает специальной привилегией смены владельца на другого пользователя, обладающего такой же специальной привилегией (например, на самого себя).

Разграничение доступа к файлам и папкам возможно с помощью Проводника Windows (вкладки Безопасность функций Свойства контекстного меню выделенного объекта), принтеру – с помощью функции Принтеры и факсы Панели управления (вкладки Безопасность функции Свойства выделенного принтера), реестру Windows – с помощью Редактора реестра regedit.exe (функции Разрешения контекстного меню выделенного раздела).

Права доступа к объектам в операционной системе Windows делятся на специальные, стандартные (общие) и родовые (generic). Специальные права зависят от типа объекта разграничения доступа. Например, к файлам и папкам могут применяться следующие специальные права:

– обзор папок (выполнение файлов);

– содержание папки (чтение данных из файла);

– чтение атрибутов;

– чтение дополнительных атрибутов;

– создание файлов (запись данных в файл);

– создание папок (дозапись данных в файл);

– запись атрибутов;

– запись дополнительных атрибутов;

– удаление подпапок и файлов (только для папок).

Стандартные права доступа к объектам операционной системы Windows не зависят от типа объекта. Определены следующие стандартные права доступа;

– удаление;

– чтение разрешений;

– смена разрешений (для реестра это право названо Запись DAC);

– смена владельца;

– синхронизация (для реестра это право названо Уведомление).

Каждое из родовых разрешений представляет собой логическую группу специальных и стандартных разрешений. Например, для файлов и папок родовое право доступа «Изменение» включает все разрешения кроме «Удаление подпапок и файлов», «Смена разрешений» и «Смена владельца».

Существующий в Windows механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

Если требуется предотвратить наследование разрешений, при настройке особых (отличающихся от родовых) разрешений на доступ к родительской папке (разделу реестра) можно выбрать режим «Применять эти

разрешения к объектам и контейнерам только внутри этого контейнера». В случаях, когда необходимо отменить наследование разрешений только для некоторых файлов или подпапок (подразделов реестра), можно отменить режим «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне».

Запрещение права доступа имеет более высокий приоритет, чем его разрешение, если только объект не наследует от различных папок противоречащие друг другу значения этих параметров. В таких случаях в силу вступает значение, унаследованное от родительского контейнера, ближайшего к объекту в иерархической структуре. Дочерние объекты наследуют только наследуемые разрешения.

К вновь созданным в сеансе пользователя объектам права доступа в Windows назначаются одним из следующих способов:

1. На основе явно заданного субъектом (управляемой пользователем программой) и корректного по форме дескриптора безопасности (например, при вызове системных функций CreateFile или CreateDirectory при создании файлов или папок);

2. На основе механизма наследования (если при создании объекта дескриптор безопасности не задается);

3. Из полученного при начале сеанса маркера доступа субъекта, создающего объект (если наследование невозможно).

Индекс файла в Linux содержит информацию о владельце файла (его идентификаторе, User Identifier, UID), его первичной группе (идентификаторе группы, GroupIdentifier, GID) и векторе доступа к файлу. В отличие от Windows вектор доступа в Linux состоит всегда из трех элементов, определяющих права доступа к объекту трех категорий субъектов (владельца, членов его группы и всех остальных). Суперпользователь в Linux имеет полные, никем не ограничиваемые права доступа к любому объекту.

В Linux существуют только три права доступа – чтение, запись и выполнение. Для каталогов право чтения означает разрешение на просмотр содержания каталога, право записи – разрешение создания, добавления и удаления файлов в каталоге, право выполнения – разрешение на поиск файла в каталоге по его имени.

Ограниченность прав доступа к объектам в ОС Linux вынуждает использовать так называемые дополнительные биты доступа в каждой из его частей:

– SUID (дополнительный бит доступа в подвекторе прав владельца). Обеспечивает выполнение файла с правами не пользователя, а владельца файла (необходимо, например, для предоставления права записи в файл учетных записей /etc/passwd непривилегированному пользователю при смене им своего пароля).

– SGID (дополнительный бит в подвекторе прав членов группы владельца файла). Обеспечивает выполнение файла с правами не пользователя, а членов группы владельца файла.

– Sticky (дополнительный бит в подвекторе прав всех остальных пользователей). Запрещает удаление и переименование в общем каталоге файлов, созданных другими пользователям.

Управлять значением вектора доступа к вновь созданным в сеансе пользователя файлам в ОС Linux администратор может с помощью системной переменнойumask, значение которой может устанавливаться в файлах пользователей .login, .cshrc или .profile либо в системном файле / etc / profile. Значение umask определяет сбрасываемые биты в элементах вектора доступа к создаваемому объекту.

Сравнивая реализацию дискреционного разграничения доступа к объектам в операционных системах Microsoft Windows и Linux, можно отметить следующее:

– Использование привилегии администратора Windows «Овладение файлами или иными объектами» более безопасно, чем работа в Linux с правамисуперпользователя, но менее удобна с точки зрения простоты администрирования.

– Большое количество разнообразных прав доступа к объектам в Windows увеличивает гибкость механизма управлении доступом, но повышает риск ошибочного наделения пользователя или группы избыточными правами доступа.

– В Linux администратору проще управлять правами доступа к объектам, создаваемым пользователем в ходе своей работы в системе.

– В Windows возможно назначение индивидуальных прав доступа к объекту для любого отдельно взятого пользователя или группы.

В расширении подсистемы разграничения доступа к файлам для операционной системы Linux − Linux ACLs – реализована возможность настроить индивидуальные права доступа к файлам «с точностью» до отдельного пользователя.

В расширении базовой модели безопасности операционной системы Linux (Security-Enhanced Linux − Linux с улучшенной безопасностью, SELinux) реализовано мандатное разграничение доступа к объектам в рамках модели домен-тип. В этой модели каждый процесс запускается в определённом домене безопасности (с определенным уровнем допуска), а всем объектам ставится в соответствие определённый тип (метка секретности).

Список правил, ограничивающих возможности доступа доменов к типам, называется политикой и задаётся один раз в момент установки системы. Описание политики в SELinux − это набор текстовых файлов, которые могут быть скомпилированы и загружены в память ядра Linux при запуске системы.

Возможности SELinux по управлению доступом значительно превосходят возможности базовых прав Unix. Например, можно строго ограничить номер сетевого порта, с которым будет связан сетевой сервер или разрешить создание и запись в файл, но не его удаление. Это позволяет ограничить системные службы с помощью явно заданного набора существующих прав.

Поддержка ролевого разграничения доступа включена в серверные операционные системы Windows и в серверную операционную систему ALT Linux Castle. Программисты и администраторы Windows-систем могут использовать преимущества ролевого разграничения доступа к объектам с помощью оснастки Диспетчер авторизации (Authorization Manager).

В соответствии с реализованной в ОС ALT Linux Castle ролевой моделью управления доступом определяются роли и типы, а затем определяется, что может делать та или иная роль с тем или иным типом [3]. Таким образом, создается некоторая абстрактная модель, которая затем связывается к реальным пользователям, программам и файлам. Независимость модели от реальных субъектов и объектов позволяет производить мгновенную перенастройку политики безопасности быстрым изменением связей ролей и (или) типов. Кроме того, это очень удобно для создания готовых решений, например, распределения ролей и типов для защиты содержимого страниц Web-узла. Интересной особенностью является возможность запуска программ с ролью, отличной от роли пользователя, производящего запуск. В результате можно, например, произвести такие настройки, что прямой доступ к диску будут иметь только разрешенные программы, а все остальные пользователи системы (включая администратора) будут лишены такой возможности.

В докладе представлены результаты сравнительного анализа средств разграничения доступа к объектам ОС Windows и Linux. Показаны

достоинства и недостатки реализаций дискреционного разграничения доступа в этих ОС, возможности ролевого управления доступом, появившиеся в их серверных версиях.

2.2. Разграничение доступа средство защиты

Разграничение доступа может быть физическим и логическим.

Физическое разграничение доступа подразумевает выделение определённых пространственных зон (территорий, помещений) и определение круга лиц, которым разрешён доступ в ту или иную зону. Например, на территорию предприятия разрешён доступ только сотрудникам предприятия. Чтобы контролировать доступ (то есть пропускать "своих" и не пропускать "чужих") существует служба охраны и проходная, оснащённая теми или иными техническими средствами. Однако на территории предприятия могут быть места, куда допускаются не все сотрудники предприятия. Например, в помещения первого отдела разрешён вход только сотрудникам этого отдела. Для ограничения доступа в такие помещения могут использовать дополнительные посты охраны, специальные кодовые замки и другие технические устройства.

Физическое разграничение доступа играет важную роль в обеспечении информационной безопасности. Необходимо ограничивать доступ посторонних лиц к компьютерам, на которых обрабатывается конфиденциальная информация, а также к компьютерам, которые имеют особое значение для бесперебойного функционирования системы (например, к серверам). Такие компьютеры лучше устанавливать в изолированных помещениях, вход в которые разрешён только тем, кто непосредственно работает на этих компьютерах.

Однако чаще под разграничением доступа имеется в виду логическое управление доступом, то есть комплекс программных средств, позволяющий специфицировать и контролировать действия, которые субъекты

(пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами).

Логическое управление доступом - основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов.

С формальной точки зрения задача управления доступом сводится к следующему. Пусть имеется совокупность субъектов (в дальнейшем для простоты под субъектами будем понимать только пользователей компьютера) и набор объектов (например, файлов на жёстком диске компьютера). Задача логического управления доступа состоит в том, чтобы для каждой пары "субъект - объект" определить множество допустимых операций (зависящее, может быть, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты - объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в пересечении строк и столбцов записаны разрешённые виды доступа и дополнительные условия.

Например, матрица доступа может выглядеть следующим образом:

	Файл А	Файл В	Линия связи
Пользователь 1	Только чтение	Только чтение	Нет доступа
Пользователь 2	Только чтение	Чтение и запись	С 10:00 до 18:00
Пользователь 3	Полный доступ	Полный доступ	Круглосуточно

После того, как права субъектов в отношении объектов определены, встаёт задача контроля соблюдения этих прав. Для этого должны существовать программные средства, которые позволяют, с одной стороны, блокировать попытку запрещённого доступа, а с другой стороны, регистрировать действия пользователей (либо действия, выполняемые над определёнными объектами).

Процесс регистрации выполняемых действий называется протоколированием. На основе анализа протоколов системы

осуществляется аудит, то есть проверка допустимости и корректности произошедших в системе событий.

Аудит позволяет выявит попытки несанкционированного доступа, отследить активность пользователей и является важной составной частью по предотвращению и расследованию случаев нарушения информационной безопасности.

Следует отметить, что для аудита может использоваться не только информация, специально регистрируемая средствами контроля доступа, но и вообще любые данные, так или иначе отражающие характер действий пользователя (дата и время создания файлов, дата и время регистрации в системе, информация в заголовках электронных писем). Следует, однако, помнить, что такая информация может быть подделана злоумышленником.Например, в 1996 году личный секретарь вице - президента компании Oracle предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина предъявила электронное письмо, якобы отправленное ей президентом компании. Однако президент предъявил файл с регистрационной информацией компании сотовой связи, из которого видно, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от рабочего места. Таким образом, в суде возникло противостояние "файл против файла". Суд решил, что подделано электронное письмо, так как секретарша знала пароль президента. Таким образом, использование системной информации в качестве доказательств в суде связано с определёнными сложностями.

Права и полномочия доступа

Права доступа определяют, какие действия субъект (пользователь), может выполнить с объектом. Набор возможных действий зависит от вида объекта. Само понятие объекта меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, папки, устройства и процессы

Например в ОС Windows существуют следующие права доступа к папкам:

· чтение (Read). Право на чтение автоматически устанавливается при открытии доступа к папке. Такое право позволяет просматривать имена файлов и папок в этой папке, просматривать данные о файле и его атрибуты; запускать программные файлы;

· изменение (Modify). Право на изменения включает в себя все права на чтение и, кроме того, позволяет добавлять файлы и другие папки, изменять данные в файлах и удалять файлы и другие папки;

· полный доступ (full control). Включает все права на чтение и изменение плюс право изменять права для файлов и папок NTFS (об NTFS см. далее).

Для принтера можно задать следующие права доступа:

· печать (Print) - можно подключаться к принтеру и рассматривать в нём документы. По умолчанию всем членам группы "Все" предоставляется право на печать;

· управление принтером (Manage Printers). Пользователь может распечатывать документы и обладает полным административным контролем над принтером. Он может приостановить работу принтера, перезагрузить его, изменить его настройки, уровни доступа к нему и права доступа;

· управление документами (Manage Documents). Пользователь может приостановить, возобновить, перезагрузить, отменить и перераспределить порядок документов, отправленных на печать остальными пользователями.

Применительно к процессам могу рассматриваться права на создание и уничтожение.

Современные операционные системы могут поддерживать и другие объекты

Для систем управления реляционными базами данных объектом может являться база данных, таблица, форма, процедура. Применительно к

таблицам могут задаваться права на операции поиска, добавления, модификации и удаления данных. У других объектов другие виды доступа.

Разнообразие объектов и применяемых к ним операций приводит к тому, что управление доступом должно осуществляться на уровне каждого конкретного сервиса.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включая в число видимых объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

Группы пользователей. Ролевое управление доступом

Группы пользователей. Формирование действующих разрешений

Каким было отмечено выше, права доступа могут храниться в матрице доступа, где для каждого пользователя определено, к каким объектам он имеет доступ, и каковы особенности этого доступа. Однако размер этой матрицы очень велик (определяется произведением числа пользователей на число объектов). Кроме того, часто многие пользователи должны иметь одинаковые права; а если права задаются для каждого пользователя, то для всех надо повторить одну и ту же процедуру установления прав.

Поэтому часто пользователей объединяют в группы. Права доступа к объектам устанавливаются всей группы. Кроме того, можно установить дополнительные права для отдельных пользователей.

Разрешения пользователя на доступ к объектам файловой системы работают по принципу дополнения (аддитивности). Это значит, что действующие разрешения, то есть те разрешения, которые пользователь реально имеет в отношении конкретного каталога или файла, образуются из всех прямых и косвенных разрешений, назначенных пользователю для данного объекта с логической функцией ИЛИ. Например, если пользователь

имеет прямо назначенное разрешение для каталога на чтение, а косвенно через членство в группе ему дано разрешение на запись, то в результате пользователь сможет читать информацию в файлах каталога и записывать в них данные.

Однако правило сложения разрешений с помощью логического ИЛИ не выполняется, когда пользователь имеет определённое разрешение, а группе в этом разрешении отказано (или наоборот). В этом случае отказ в разрешении имеет более высокий приоритет, чем предоставление разрешения, то есть в результате пользователь не будет иметь разрешения.

Ролевое управление доступом

При большом количестве пользователей традиционные системы управления доступом становятся крайне сложными для администрирования. Необходимы решения в объектно-ориентировочном стиле, способные эту сложность понизить. Таким решением является ролевое управление доступом. Суть его в том, что между пользователями и их правами появляются промежуточные сущности (роли). Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых даёт ему определённые права. С другой стороны, каждая роль может быть присвоена нескольким пользователям. Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других сервисов. В частности, существует реализации ролевого доступа для Web - серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом (http://csrc.nist.gov/rbacl). Каждой роли приписываются определённые права доступа. Например, роли "сотрудник" приписываются права просмотра информации о продукции предприятия и распоряжений администрации; а роли "бухгалтер" приписываются, кроме того, права изменения информации о зарплате сотрудников. С другой стороны, каждому пользователю во время

сеанса работы приписывается определённая роль (или несколько ролей). В соответствии с данной ролью пользователь и получает права доступа.

При ролевом управлении доступом должны соблюдаться принципы разделения обязанностей.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. Например, если пользователь приписан роли "бухгалтер", то он не может быть приписан роли "архивариус".

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, активные в течение одного сеанса пользователя. Например, один и тот же пользователь имеет право выступать и в роли "бухгалтер", и в роли "кассир", но не одновременно: чтобы стать "бухгалтером", он должен сначала закрыть кассу. Тем самым реализуется так называемое "временное ограничение доверия".

Средства разграничения доступа в ОС Windows

Права доступа к файлам. NTFS

При разработке систем Windows большое внимание уделялось средствам разграничения доступа. Эти средства совершенствовались с каждой новой ОС.

Система Windows XP имеет развитые средства ограничения доступа.

Возможность задания разных прав доступа к файлам для разных пользователей связана с использованием файловой системы NTFS.

Файловая система NTFS обладает характеристиками защищённости, поддерживая контроль доступа к данным и привилегии владельца, играющие исключительно важную роль в обеспечении целостности жизненно важных конфиденциальных данных. Папки и файлы NTFS могут иметь назначенные им права доступа вне зависимости от того, являются они общими или нет. NTFS позволяет назначать права доступа к отдельным файлам. Однако, если файл будет скопирован из раздела NTFS в раздел FAT, все права доступа и другие уникальные атрибуты, присущие NTFS, будут

утрачены. NTFS обеспечивает такое сочетание производительности, надёжности и эффективности, какого невозможно добиться с помощью FAT.

Основными целями разработки NTFS являлись обеспечение скоростного выполнения стандартных операций над файлами (включая чтение, запись) и предоставление дополнительных возможностей, включая сжатие и восстановление повреждённых файлов. Помимо разграничения доступа, NTFS поддерживает шифрование файлов с помощью EFS (Encrypting File System).

Для каждого пользователя или группы можно назначить или запретить стандартные разрешения для файлов: полный доступ (full control), изменение (modyfy), чтение и выполнение (read & execute), чтение (read) и запись (write). Для установок разрешения или отказа служат флажки Разрешить (Allow) и Запретить (Deny).

Для папок разрешения устанавливается аналогичным образом.

Учетные записи

Чтобы "понять", имеет ли определённый пользователь права доступа по отношению к конкретному объекту, система должна каким - либо образом идентифицировать каждого пользователя. Для этого используются учётные записи пользователей и групп. Создание учётных записей занимает важное место в обеспечении безопасности Windows XP, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации, разрешать или запрещать выполнение определённых действий. Для регистрации пользователя в системе Windows XP в обязательном порядке требуется наличие пользовательской учётной записи (user account). Причём пользователь идентифицируется не по входному имени и паролю (login/password), а по идентификатору безопасности (Security ID, SID). Большинство идентификаторов безопасности являются уникальными для каждого пользователя (в том числе и для пользовательских учётных записей

в разных системах). Исключение составляют только так называемые "хорошо известные" SID, например, такие как встроенная группа Everyone (Все).

Сразу после установки системы Windows XP автоматически создаются встроенные учётные записи:

· Administrator (Администратор) - используется при установке рабочей станции или сервера, являющегося членом домена. Эта запись не может быть уничтожена, блокирована или удалена из группы Администратора

· Guest (Гость) - учётная запись для регистрации в системе без специально созданной учётной записи. она не требует ввода пароля и по умолчанию заблокирована

· HepAssistaint - используется при работе средства Remote Assistance; по умолчанию заблокирована

·Support - 38894500 – зарезервирована для поддержки справочной службы Microsoft; по умолчанию заблокирована

Автоматически создаются также встроенные группы:

·Administrators (Администраторы) - обладают полным доступом ко всем ресурсам системы

·BackupOperations (Операторы архива) - могут восстанавливать и архивировать файлы

· Guests (Гости) - могут зарегистрироваться в системе и получать ограниченные права

·owerUsers (Опытные пользователи) - обладают большими правами, чем члены групп Guests и Users

· Replicators (Репликатор) - специальная группа для работы в сети

· Users (Пользователи) - могут выполнять большинство пользовательских функций

· А также:

· Network Configuration Operatons (Операторы настройки сети),

· Remote Desktop Users (Удаление пользователей рабочего стола),

· Help Services Group (Группа Служб Поддержки).

В процессе работы в системе могут создаваться новые группы и пользовательские учётные записи; может меняться членство пользователей в локальных группах.

2.3. Методы разграничения доступа к сетевым приложениям

Широкое применение информационных технологий создало проблемы не только производительности, надежности и устойчивости функционирования информационных систем, а также проблемы защиты циркулирующей в системах информации от несанкционированного доступа.

Риски, которые несут современные предприятия в связи с несанкционированным использованием данных и приложений, сделали этот фактор одной из наиболее опасных угроз при работе с информацией. Таким образом, на одно из первых мест в информационной безопасности вышла проблема защиты от несанкционированного доступа (НСД), подразумевающая возможность работать в условиях безопасности, как с открытыми, так и с конфиденциальными данными.

К видам НСД относят атаки на корпоративную сеть извне, доступ сотрудников к конфиденциальной информации, несанкционнированое чтение или копирование посторонними данных, принадлежащих компании. Типовыми сценариями НСД могут стать просмотр, копирование, искажение и уничтожение данных, перехват и блокирование информации, подмена процессов обработки данных и т. д.

В связи с этим именно АРМ (автоматизированное рабочее место), находящийся в составе сети, следует в первую очередь рассматривать в качестве объекта защиты, а конечного пользователя – в качестве ее наиболее вероятного потенциального нарушителя.

Для предупреждения несанкционированного доступа к информации применяют технологии идентификации, аутентификации, авторизации и

аудита. После выполнения идентификации и аутентификации необходимо установить полномочия субъекта для последующего контроля санкционированного использования вычислительных ресурсов, доступных в сети предприятия. Такой процесс называется разграничением доступа. Обычно выделяют следующие методы разграничения доступа:

- дискреционная модель разграничения доступа;
- ролевое разграничение доступа;
- модель информационных потоков;
- мандатная модель разграничения доступа.

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретных пользователей или групп. Эта модель отличается простотой реализации. Ролевое разграничение доступа является развитием дискреционной модели разграничения доступа; при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Задание ролей позволяет определить более четкие и понятные для пользователей информационной системы правила разграничения доступа. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа. На основе ролевого разграничения доступа, в том числе, может быть реализовано мандатное разграничение доступа.

Мандатная модель разграничения доступа предполагает назначение объекту грифа секретности, а субъекту – уровня допуска. Чаще всего мандатную модель описывают в терминах, понятиях и определениях свойств модели Белла-ЛаПадула. Доступ субъектов к объектам в мандатной модели определяется на основании правил «не читать выше» и

«не записывать ниже». Это означает, что пользователь не может прочитать информацию из объекта, гриф секретности которого выше, чем его уровень допуска. Также пользователь не может перенести информацию из объекта с большим грифом секретности в объект с меньшим грифом секретности. Использование мандатной модели предотвращает утечку конфиденциальной информации, но снижает производительность программно-аппаратной системы.

Модель безопасности информационных потоков в большинстве случаев используется в сочетании с моделью другого вида, например с дискреционной или мандатной. Реализация модели безопасности информационных потоков, как правило, на практике является трудной для решения задачей, особенно, если необходимо обеспечить защиту компьютерной системы от возникновения неблагоприятных информационных потоков по времени.

Но рассмотренные выше методы имеют ряд недостатков. Дискреционная модель представляет собой достаточно примитивную, хотя и простую для описания модель логического разграничения доступа, построенные на ней системы получаются громоздкими и непонятными. Мандатная модель разграничения доступа на основе упорядоченных меток безопасности является, наоборот, слишком жесткой с точки зрения условий, которые она реализует, удобной в верификации, простой в представлении и настройке, однако пригодной для весьма узкого класса информационных систем. Ролевая модель сопряжена с большими трудностями внедрения дополнительных механизмов в ядра операционных систем и их использованием в составе программных комплексов.

Исходя из указанных недостатков, существует потребность в создании универсального программного обеспечения для разграничения доступа к данным, которое будет предоставлять возможность самому

определить модель разграничения доступа, лучше всего подходящую под нужды защищаемого информационно-вычислительного комплекса. Создание именно такого программного обеспечения я и поставила целью своей дипломной работы. В данном средстве будет применена политика, позволяющая гибко формировать разграничение прав доступа в соответствии с нуждами предприятия.

Заключение

Создание роли может быть выполнено только пользователем, имеющим специальную системную привилегию. Для того, чтобы предоставить пользователю некоторую роль, необходимо создать эту роль и разрешить ее в текущем сеансе. Управление разрешением или запрещением ролей в текущем сеансе выполняется специальной командой. До тех пор пока явно не будет разрешено использование роли в сеансе, привилегии, определенные для пользователя ролью, не предоставляются. Обычно команда активизации роли подобно операторным скобкам устанавливает корректный домен полномочий пользователя для проведения логически единого с точки зрения разграничения доступа действия.

Для управления системой разграничения доступа на основе концепции глобальных ролей и глобальных пользователей разработано пециализированное средство – сервер безопасности (Oracle Security Server). Оно включает централизованный сервер, управляющий специализированной базой данных (репозиторием), распределенные компоненты администратора и адаптеры безопасности. Адаптеры безопасности, входящие в программное обеспечение слоев уровня представления всех клиентов и серверов, позволяют устанавливать подлинность взаимодействующих элементов распределенной системы и получать информацию о подлинности и допустимости используемых глобальных ролей.

Список литературы

1. Разграничение доступа к информации в компьютерных системах/ Н. А. Гайдамакин/М./2005

2. SELinux: теория и практика безопасности. http://www.interface.ru/ home.asp?artId=2699.

3. Хорев П.Б. Ролевое управление доступом к ресурсам в операционной системе Microsoft Windows Server 2003. Труды XVI международной научно-технической конференции «Информационные средства и технологии». В 3 томах. Т. 2. М.: Издательский дом МЭИ, 2008. С. 80-88.

4. ALTLinux Castle. Общие сведения.

5. http://www.linuxcenter.ru/ lib/articles/distrib/altlinux/castle.phtml.