ЧАСТЬ 6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

19. СРЕДСТВА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В АРХИТЕКТУРЕ ОПЕРАЦИОННЫХ СИСТЕМ WINDOWS

19.1 Средства управления безопасностью

Для управления системой безопасности в ОС Windows имеются разнообразные и удобные инструментальные средства. В частности, потребуется умение управлять учетными записями пользователей при помощи панели «Пользователи и пароли». Кроме того понадобится контролировать привилегии пользователей при помощи панели «Назначение прав пользователям». Рекомендуется также освоить работу с утилитой просмотра данных маркера доступа процесса WhoAmI.exe, утилитами просмотра и редактирования списков контроля доступа (cacls.exe, ShowACLs.exe, SubInACL,exe, SvcACL.exe), утилитой просмотра маркера доступа процесса PuList.exe и рядом других.

19.1.1 Система управления доступом

Подсистема защиты данных является одной из наиболее важных. В центре системы безопасности ОС Windows находится система контроля доступа.

С каждым процессом или потоком, то есть активным компонентом (**субъектом**), связан маркер доступа, а у каждого защищаемого объекта (например, файла) имеется дескриптор защиты. Проверка прав доступа обычно осуществляется в момент открытия объекта и заключается в сопоставлении прав **субъекта** списку прав доступа, который хранится в составе дескриптора защиты **объекта**

Защищаемые объекты Windows включают:

- файлы,
- устройства,
- каналы,
- события,
- мьютексы,
- семафоры,
- разделы общей памяти,
- разделы реестра
- и другое. *Сущность, от которой нужно защищать объекты, называется*

«субъектом». Субъектами в Windows являются процессы и потоки, запускаемые конкретными пользователями. *Субъект безопасности - активная системная составляющая, а объект - пассивная.*

Помимо дискреционного доступа Windows поддерживает управление ***привилегированным*** **доступом**. Это означает, что в системе имеется пользователь-администратор с неограниченными правами.

Кроме того, для упрощения администрирования пользователи Windows объединены в **группы**. Пользователь, как член группы, облекается, таким образом, набором полномочий, необходимых для его деятельности, и играет определенную роль. Подобная стратегия называется **управление *ролевым* доступом.**

Ключевая цель системы защиты Windows - *следить за тем, кто и к каким объектам осуществляет доступ.* Система защиты хранит информацию, относящуюся к безопасности для каждого пользователя, группы пользователей и объекта. Модель защиты ОС Windows требует, чтобы субъект на этапе открытия объекта указывал, какие операции он собирается выполнять в отношении этого объекта.

Единообразие контроля доступа *к различным объектам (процессам, файлам, семафорам и др.) обеспечивается тем, что с каждым процессом (потоком) связан маркер доступа, а с каждым объектом - дескриптор защиты. Маркер доступа в качестве параметра имеет идентификатор пользователя, а дескриптор защиты - списки прав доступа. ОС может контролировать попытки доступа, которые прямо или косвенно производятся процессами и потоками, инициированными пользователем.*

19.1.2 Пользователи и группы пользователей

Каждый пользователь (и каждая группа пользователей) системы должен иметь учетную запись (account) в базе данных системы безопасности. Учетные записи идентифицируются именем пользователя и хранятся в базе данных SAM (Security Account Manager) в разделе HKLM/SAM реестра.

Учетная запись пользователя содержат набор сведений о пользователе, такие, как имя, пароль (или реквизиты), комментарии и адрес.

Наиболее важными элементами учетной записи пользователя являются:

1. список привилегий пользователя в отношении данной системы,
2. список групп, в которых состоит пользователь,
3. идентификатор безопасности **SID** (Security IDentifier).

Идентификаторы безопасности генерируются при создании учетной записи. Они (а не имена пользователей, которые могут не быть уникальными) служат основой для идентификации субъектов внутренними процессами ОС Windows.

Учетные записи групп, созданные для упрощения администрирования, содержат список учетных записей пользователей, а также включают сведения, аналогичные сведениям учетной записи пользователя (SID группы, привилегии члена группы и др.).

SID пользователя (и группы) является уникальным внутренним идентификатором и представляют собой структуру переменной длины с коротким заголовком, за которым следует длинное случайное число. Это числовое значение формируется из ряда параметров, причем утверждается, что вероятность появления двух одинаковых SID практически равна нулю. В частности, если удалить пользователя в системе, а затем создать его под тем же именем, то SID вновь созданного пользователя будет уже другим.

Узнать свой идентификатор безопасности пользователь легко может при помощи утилит *whoami* или *getsid* из ресурсов Windows.

Система хранит идентификаторы безопасности в бинарной форме, однако существует и текстовая форма представления SID. Текстовая форма используется для вывода текущего значения SID, а также для интерактивного ввода (например, в реестр).

В текстовой форме каждый идентификатор безопасности имеет определенный формат. Вначале находится префикс S, за которым следует группа чисел, разделенных дефисами. Например, SID администратора системы имеет вид: *S-1-5-<домен>-500*, а SID группы everyone, в которую входят все пользователи, включая анонимных и гостей - *S-1-1-0*.

19.1.3 Объекты. Дескриптор защиты

В ОС Windows все типы объектов защищены одинаковым образом. С каждым объектом связан ***дескриптор защиты*** *(security descriptor)*. Связь объекта с дескриптором происходит в момент создания объекта.

Дескриптор защиты (см. рис. 19.1) содержит

- SID владельца объекта,
- SID групп для данного объекта
- два указателя на списки DACL (Discretionary ACL) и SACL (System ACL) контроля доступа.

DACL и SACL содержат разрешающие и запрещающие доступ списки пользователей и групп, а также списки пользователей, чьи попытки доступа к данному объекту подлежат аудиту.

Структура каждого ACL списка проста. Это набор записей ACE (Access Control Entry), каждая запись содержит SID и перечень прав, предоставленных субъекту с этим SID.

На примере, изображенном на рис. 19.1, владелец файла Александр имеет право на все операции с данным файлом, всем остальным обычно дается только право на чтение, а Павлу запрещены все операции. Таким образом, ***список DACL*** *описывает все права доступа к объекту*. Если этого списка нет, то все пользователи имеют все права; если этот список существует, но он пустой, права имеет только его владелец.

Рис. 19.1 - Структура дескриптора защиты для файла

В списке ACL есть записи ACE двух типов:

- *разрешающие доступ.* Разрешающая запись содержит SID пользователя или группы и битовый массив (access mask), определяющий набор операций, которые процессы, запускаемые этим пользователем, могут выполнять с данным объектом.
- *запрещающие доступ*. Запрещающая запись действует аналогично, но в этом случае процесс не может выполнять перечисленные операции.

Кроме списка DACL дескриптор защиты включает также список SASL, который имеет такую же структуру, что и DACL, то есть состоит из таких же ACE записей, только вместо операций, регламентирующих доступ к объекту, в нем перечислены операции, подлежащие аудиту.

В примере на рис. 19.1 операции с файлом процессов, запускаемых пользователем Сергеем, описанные в соответствующем битовом массиве будут регистрироваться в системном журнале.

19.1.4 Субъекты безопасности. Процессы, потоки. Маркер доступа

Так же как и объекты, субъекты должны иметь отличительные признаки - контекст пользователя, для того, чтобы система могла контролировать их действия. Сведения о контексте пользователя хранятся в маркере (употребляются также термины «токен», «жетон») доступа.

При интерактивном входе в систему пользователь обычно вводит свое имя и пароль. Система (процедура Winlogon) по имени находит соответствующую учетную запись, извлекает из нее необходимую информацию о пользователе, формирует список привилегий,

ассоциированных с пользователем и его группами, и все это объединяет в структуру данных, которая называется маркером доступа.

Маркер также хранит некоторые параметры сессии, например, время окончания действия маркера. Таким образом, именно маркер является той визитной карточкой, которую субъект должен предъявить, чтобы осуществить доступ к какому-либо объекту.

Основные компоненты маркера доступы показаны на рис. 19.2.

SID пользова-теля	SIDi, ... SIDn Идентификаторы групп пользователя	DACL по умолчанию	Привиле-гии	Другие параметры

Рис. 19.2 - Основные компоненты маркера доступа

Включая в маркер информацию о защите, в частности, DACL, Windows упрощает создание объектов со стандартными атрибутами защиты. Как уже говорилось, если процесс не позаботится о том, чтобы явным образом указать атрибуты безопасности объекта, на основании списка DACL, присутствующего в маркере, будут сформированы права доступа к объекту по умолчанию.

19.1.5 Проверка прав доступа

После формализации атрибутов защиты субъектов и объектов можно перечислить основные этапы проверки прав доступа см. рис. 19.3.

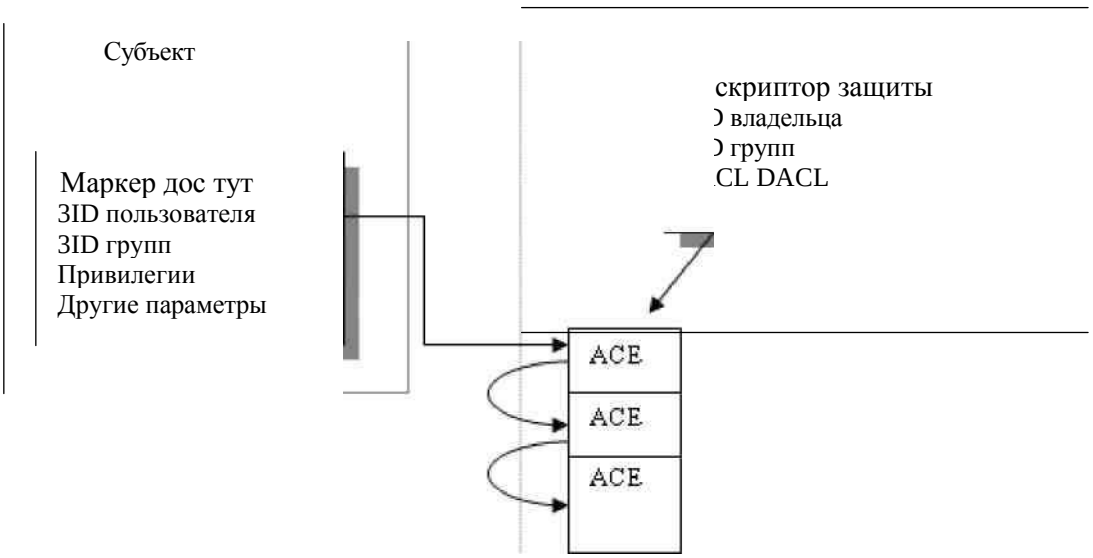

Рис. 19.3. - Пример проверки прав доступа к защищенному объекту

Этапов проверки довольно много. Наиболее важные этапы из них:

- Если SID субъекта совпадает с SID владельца объекта и запрашиваются стандартные права доступа, то доступ предоставляется независимо от содержимого DACL.
- Далее система последовательно сравнивает SID каждого ACE из DACL с SID маркера. Если обнаруживается соответствие, выполняется сравнение маски доступа с проверяемыми правами. Для запрещающих ACE даже при частичном совпадении прав доступ немедленно отклоняется. Для успешной проверки разрешающих элементов необходимо совпадение всех прав.

Очевидно, что для процедуры проверки важен порядок расположения ACE в DACL. Поэтому Microsoft предлагает так называемый предпочтительный порядок размещения ACE. Например, для ускорения рекомендуется размещать запрещающие элементы перед разрешающими.

19.2 Основные компоненты системы безопасности

Система контроля дискреционного доступа - центральная концепция защиты ОС Windows, однако перечень задач, решаемых для обеспечения безопасности, этим не исчерпывается. В данном разделе будут проанализированы структура, политика безопасности и API системы защиты.

Изучение структуры системы защиты помогает понять особенности ее функционирования. Несмотря на слабую документированность ОС Windows по косвенным источникам можно судить об особенностях ее функционирования.

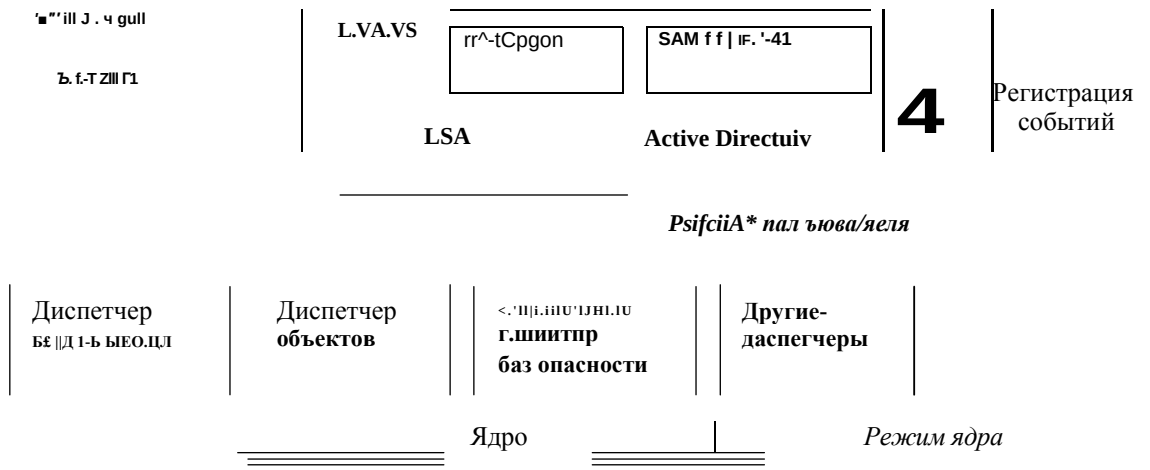

Рис. 19.4 - Структура системы безопасности ОС Windows

Система защиты ОС Windows состоит из следующих компонентов (см. рис. 14.1).

- **Процедура регистрации (Logon Processes),** которая обрабатывает запросы пользователей на вход в систему. Она включают в себя

начальную интерактивную процедуру, отображающую начальный диалог с пользователем на экране, и удаленные процедуры входа, которые позволяют удаленным пользователям получить доступ с рабочей станции сети к серверным процессам Windows NT. Процесс *Winlogon* реализован в файле Winlogon.exe и выполняется как процесс пользовательского режима. Стандартная библиотека аутентификации *Gina* реализована в файле *Msgina.dll*.

- **Подсистема локальной авторизации (Local Security Authority, LSA)**, которая гарантирует, что пользователь имеет разрешение на доступ в систему. Этот компонент - центральный для системы защиты Windows NT. Он порождает маркеры доступа, управляет локальной политикой безопасности и предоставляет интерактивным пользователям аутентификационные услуги. LSA также контролирует политику аудита и ведет журнал, в котором сохраняются сообщения, порождаемые диспетчером доступа. Основная часть функциональности реализована в *Lsasrv.dll*.
- **Менеджер учета (Security Account Manager, SAM)**, который управляет базой данных учета пользователей. Эта база данных содержит информацию обо всех пользователях и группах пользователей. Данная служба реализована в *Samsrv.dll* и выполняется в процессе *Lsass*.
- **Диспетчер доступа (Security Reference Monitor, SRM)**, проверяющий, имеет ли пользователь право на доступ к объекту и на выполнение тех действий, которые он пытается совершить. Этот компонент обеспечивает легализацию доступа и политику аудита, определяемые LSA. Он предоставляет услуги для программ супервизорного и пользовательского режимов, чтобы гарантировать, что пользователи и процессы, осуществляющие попытки доступа к объекту, имеют необходимые права. Данный компонент также порождает сообщения службы аудита, когда это необходимо. Это компонент исполнительной системы: Ntoskrnl.exe.

Все компоненты активно используют базу данных Lsass, содержащую параметры политики безопасности локальной системы, которая хранится в разделе HKLM\SECURITY реестра.

Реализация модели дискреционного контроля доступа связана с наличием в системе одного из ее важнейших компонентов - монитора безопасности.

Монитор безопасности - *особый вид субъекта, который активизируется при каждом доступе и в состоянии отличить легальный доступ от нелегального и не допустить последний.* Монитор безопасности входит в состав диспетчера доступа (SRM), который, согласно описанию, обеспечивает также управление ролевым и привилегированным доступом.

19.2.1 Политика безопасности

Система безопасности ОС Windows отвечает требованиям класса С2 «оранжевой» книги и требованиям стандарта Common Criteria, которые составляют основу *политики безопасности системы*.

Политика безопасности подразумевает ответы на следующие вопросы:

- какую информацию защищать,
- какого рода атаки на безопасность системы могут быть предприняты,
- какие средства использовать для защиты каждого вида информации.

Требования, предъявляемые к системе защиты.

- Каждый пользователь должен быть идентифицирован уникальным входным именем и паролем для входа в систему. Доступ к компьютеру предоставляется лишь после аутентификации. Должны быть предприняты меры предосторожности против попытки против применения фальшивой программы регистрации (механизм безопасной регистрации).
- Система должна быть в состоянии использовать уникальные идентификаторы пользователей, чтобы следить за их действиями. Владелец ресурса (например, файла) должен иметь возможность контролировать доступ к этому ресурсу.
- Управление доверительными отношениями. Необходима поддержка наборов ролей (различных типов учетных записей). Кроме того, в системе должны быть средства для управления привилегированным доступом.
- ОС должна защищать объекты от повторного использования. Перед выделением новому пользователю все объекты, включая память и файлы, должны быть проинициализированы.
- Системный администратор должен иметь возможность учета всех событий, относящихся к безопасности (аудит безопасности).
- Система должна защищать себя от внешнего влияния или навязывания, такого, как модификация загруженной системы или системных файлов, хранимых на диске.

Надо отметить, что, в отличие от большинства операционных систем, ОС Windows была изначально спроектирована с учетом требований безопасности, и это является ее несомненным достоинством. Посмотрим теперь, как в рамках данной архитектуры обеспечивается выполнение требований политики безопасности.

19.2.2 Ролевой доступ. Привилегии

С целью гибкого управления системной безопасностью в ОС Windows реализовано **управление доверительными отношениями (trusted facility management)**, которое требует поддержки набора ролей (различных типов

учетных записей) для разных уровней работы в системе. В системе имеется **управление привилегированным доступом**, то есть функции администрирования доступны только одной группе учетных записей - Administrators (Администраторы.).

В соответствии со своей ролью каждый пользователь обладает определенными ***привилегиями*** **и** ***правами*** на выполнение различных операций в отношении системы в целом, например, право на изменение системного времени или право на создание страничного файла. Аналогичные права в отношении конкретных объектов называются ***разрешениями***. И права, и привилегии назначаются администраторами отдельным пользователям или группам как часть настроек безопасности.

Каждая привилегия имеет следующие представления:

- дружественное имя, отображаемое в пользовательском интерфейсе Windows,
- программное имя, используемое приложениями,
- Luid - внутренний номер привилегии в конкретной системе.

Помимо привилегий в Windows имеются близкие к ним права учетных записей.

Важно, что даже администратор системы по умолчанию обладает далеко не всеми привилегиями. Это связано с **принципом предоставления минимума привилегий**. В каждой новой версии ОС Windows, в соответствии с этим принципом, производится ревизия перечня предоставляемых каждой группе пользователей привилегий, и общая тенденция состоит в уменьшении их количества. С другой стороны общее количество привилегий в системе растет, что позволяет проектировать все более гибкие сценарии доступа.

Назначение и отзыв привилегий - прерогатива **локального администратора безопасности** LSA (Local Security Authority), поэтому, чтобы программно назначать и отзывать привилегии, необходимо применять функции LSA.

Локальная политика безопасности системы *означает наличие набора глобальных сведений о защите, например, о том, какие пользователи имеют право на доступ в систему, а также о том, какими они обладают правами.* Поэтому говорят, что каждая система, в рамках которой действует совокупность пользователей, обладающих определенными привилегиями в отношении данной системы, является объектом политики безопасности. Объект политики используется для контроля базы данных LSA. Каждая система имеет только один объект политики, который создается администратором LSA во время загрузки и защищен от несанкционированного доступа со стороны приложений.

Управление привилегиями пользователей включает в себя задачи перечисления, задания, удаления, выключение привилегий и ряд других.