Тема 14. Средства обеспечения безопасности

Средства безопасности в Windows представляют собой отдельную подсистему, которая обеспечивает защиту не только файлов, но и других типов системных объектов. Файлы и каталоги NTFS представляют собой наиболее типичные примеры защищаемых объектов.

Важным элементом любой системы защиты данных является процедура входа в систему, при которой выполняется аутентификация пользователя. Система ищет введенное имя пользователя сначала в списке пользователей данного компьютера, а затем и на других компьютерах текущего домена локальной сети. В случае, если имя найдено и пароль совпал, система получает доступ к учетной записи (account) данного пользователя.

На основании сведений из учетной записи пользователя система формирует структуру данных, которая называется маркером доступа (access token). Маркер содержит идентификатор пользователя (SID, Security IDentifier), идентификаторы всех групп, в которые включен данный пользователь, а также набор привилегий, которыми обладает пользователь.

Привилегиями называются права общего характера, не связанные с конкретными объектами. К числу привилегий, доступных только администратору, относятся, например, права на установку системного времени, на создание новых пользователей, на присвоение чужих файлов. Некоторые привилегии обычно предоставляются всем пользователям (например, такие, как право отлаживать процессы, право получать уведомления об изменениях в файловой системе).

В дальнейшей работе, когда пользователю должен быть предоставлен доступ к каким-либо защищаемым ресурсам, решение о доступе принимается на основании информации из маркера доступа.

Для любого защищаемого объекта Windows (файла, каталога, диска, устройства, семафора, процесса и т.п.) может быть задана специальная структура данных – атрибуты защиты.

Основным содержанием атрибутов защиты является другая структура – дескриптор защиты. Этот дескриптор содержит следующие данные:

- идентификатор защиты (SID) владельца объекта;
- идентификатор защиты первичной группы владельца объекта;
- пользовательский («дискреционный», «разграничительный») список управления доступом (DACL, Discretionary Access Control List);
- системный список управления доступом (SACL, System Access Control List).

Пользовательский список управляет разрешениями и запретами доступа к данному объекту. Изменять этот список может только владелец объекта.

Системный список управляет только аудитом доступа данному объекту, т.е. задает, какие действия пользователей по отношению к данному объекту должны быть запротоколированы в системном журнале. Изменять этот список может только пользователь, имеющий права администратора системы.

В Windows, в отличие от многих других ОС, администратор не всесилен. Он не может запретить или разрешить кому бы то ни было, даже самому себе, доступ к чужому файлу. Другое дело, что администратор имеет право объявить себя владельцем любого файла, но потом он не сможет вернуть файл прежнему хозяину. Подобные ограничения вытекают из понимания, что администратор тоже не всегда ангел и, хотя он должен иметь в системе большие права, его действия следует хоть как-то контролировать.

Оба списка управления доступом имеют одинаковую структуру, их основной частью является массив записей управления доступом (ACE, Access Control Entity).

Структура записи ACE содержит:

- тип ACE, который может быть одним из следующих: разрешение, запрет, аудит;
- флаги, уточняющие особенности действия данной ACE;
- битовая маска видов доступа, указывающая, какие именно действия следует разрешить, запретить или подвергнуть аудиту;
- идентификатор (SID) пользователя или группы, чьи права определяет данная ACE.

Когда пользователь запрашивает доступ к объекту (т.е., например, программа, запущенная этим пользователем, вызывает функцию открытия файла), происходит проверка прав доступа. Она выполняется на основе сравнения маркера доступа пользователя со списком DACL. Система просматривает по порядку все записи ACE из DACL, для каждой ACE определяет записанный в ней SID и сверяет, не является ли он идентификатором текущего пользователя или одной из групп, куда входит этот пользователь. Если нет, то данная ACE не имеет к нему отношения и не учитывается. Если да, то выполняется сравнение прав, необходимых пользователю для выполнения запрошенной операции с маской видов доступа из ACE. При этом права анализируются весьма детально: например, открытие файла на чтение подразумевает наличие прав на чтение данных, на чтение атрибутов (в том числе владельца и атрибутов защиты), на использование файла как объекта синхронизации.

Если в запрещающей ACE найдется хотя бы один единичный бит в позиции, соответствующей одному из запрошенных видов доступа, то вся операция, начатая пользователем, считается запрещенной и дальнейшие проверки не производятся.

Если такие биты будут найдены в разрешающей ACE, то проверка следующих ACE выполняется до тех пор, пока не будут разрешены и все остальные запрошенные виды доступа.

Список DACL со всеми необходимыми разрешениями и запретами может быть установлен программно при создании файла, а впоследствии программно же может быть изменен владельцем. Можно также изменять разрешения в диалоге, воспользовавшись окном свойств файла.