Слабость метода DAC

Остановимся на этом подробнее.

Пользователь осуществляет доступ к объектам операционной системы не непосредственно, а с помощью прикладных процессов, которые запускаются от его имени. Вход пользователя в систему порождает *процесс-оболочку*, который поддерживает диалог с пользователем и запускает для него другие процессы. Процесс-оболочка получает от пользователя символьное имя и пароль и находит по ним числовые идентификаторы пользователя и его групп. Эти идентификаторы связываются с каждым процессом, запущенным оболочкой для данного пользователя. Говорят, что *процесс выступает от имени* данного пользователя или данных групп пользователей. В наиболее типичном случае любой порождаемый процесс наследует идентификаторы пользователя и групп от процесса-родителя.

Такой способ наследования прав выявляет врожденный *изъян* DAC-метода и делает систему уязвимой для атаки типа «Троянский конь». Рассмотрим пример. Если один пользователь обладает правами на доступ к файлу TopSecret с секретными данными, а другой – нет, то последний может поступить следующим образом. Он может разработать для этих целей специальную программу, имеющую самое невинное назначение, например системную утилиту. Однако, кроме своей явной функции, эта утилита делает тайную работу по копированию файла TopSecret в файл, принадлежащий злоумышленнику. Если эту программу запустит злоумышленник, то у него ничего не выйдет, так как эта утилита унаследует его права и система DAC сможет защитить файл TopSecret от несанкционированного доступа. Совсем другое дело, если злоумышленник сможет под благовидным предлогом устроить так, чтобы эту программу запустил пользователь с высоким уровнем прав. Тогда, получив необходимые привилегии, утилита с встроенным в нее «троянским конем» скопирует содержимое секретного файла в файл злоумышленника.

Это показывает, что системы с контролем доступа DAC не могут быть использованы там, где требуется очень высокий уровень защиты информации. Действительно, выполняемый на компьютере программный комплекс может включать программы, поставляемые как надежными производителями, так и менее надежными разработчиками, которым нельзя доверять на 100%. Если код программы не был подвергнут тщательной проверке на предмет наличия в ней «троянских коней», способных к копированию содержимого файлов, то тогда, какие бы строгие ограничения прав доступа не были введены, выполнение этой программы несет риск нарушения безопасности данных.