Шифрующая файловая система (EFS-Encrypting file system)

Шифрующая файловая система это тесно интегрированная с NTFS служба, располагающаяся в ядре Windows начиная с Windows 2000. Ее назначение: защита данных, хранящихся на диске, от несанкционированного доступа путем их шифрования. Появление этой службы не случайно, и ожидалось давно. Дело в том, что существующие на сегодняшний день файловые системы не обеспечивают необходимую защиту данных от несанкционированного доступа.

Единственный способ защиты от физического чтения данных это шифрование файлов. Простейший случай такого шифрования — архивирование файла с паролем. Однако здесь есть ряд серьезных недостатков. Во-первых, пользователю требуется каждый раз вручную шифровать и дешифровать (то есть, в нашем случае архивировать и разархивировать) данные перед началом и после окончания работы, что уже само по себе уменьшает защищенность данных. Пользователь может забыть зашифровать (заархивировать) файл после окончания работы, или (еще более банально) просто оставить на диске копию файла. Во-вторых, пароли, придуманные пользователем, как правило, легко угадываются. В любом случае, существует достаточное количество утилит, позволяющих распаковывать архивы, защищенные паролем. Как правило, такие утилиты осуществляют подбор пароля путем перебора слов, записанных в словаре.

Система EFS была разработана с целью преодоления этих недостатков. Ниже мы рассмотрим более подробно детали технологии шифрования, взаимодействие EFS с пользователем и способы восстановления данных, познакомимся с теорией и реализацией EFS в Windows 2000, а также рассмотрим пример шифрования каталога при помощи EFS.

Технология шифрования

EFS использует архитектуру Windows CryptoAPI. В ее основе лежит технология шифрования с открытым ключом. Для шифрования каждого файла случайным образом генерируется ключ шифрования файла. При этом для шифрования файла может применяться любой симметричный алгоритм шифрования. В настоящее же время в EFS используется один алгоритм, это DESX, являющийся специальной модификацией широко распространенного стандарта DES.

Ключи шифрования EFS хранятся в резидентном пуле памяти (сама EFS расположена в ядре Windows 2000), что исключает несанкционированный доступ к ним через файл подкачки.

Взаимодействие с пользователем

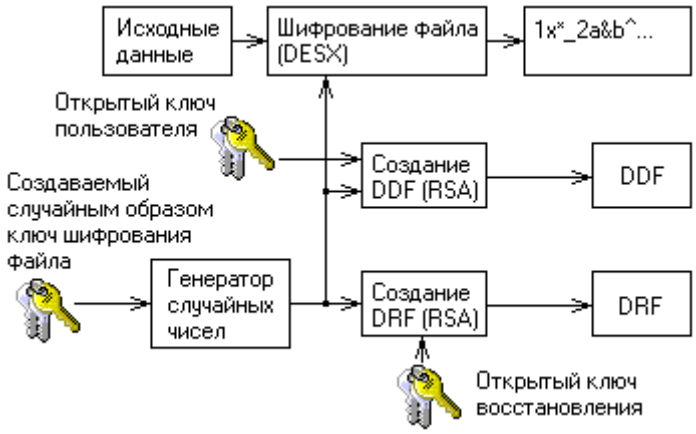
По умолчанию EFS сконфигурирована таким образом, что пользователь может сразу начать использовать шифрование файлов. Операция шифрования и обратная поддерживаются для файлов и каталогов. В том случае, если шифруется каталог, автоматически шифруются все файлы и подкаталоги этого каталога. Необходимо отметить, что если зашифрованный файл перемещается или переименовывается из зашифрованного каталога в незашифрованный, то он все равно остается зашифрованным. Операции шифрования/дешифрования можно выполнить двумя различными способами — используя Windows Explorer или консольную утилиту Cipher.

Немного теории

EFS осуществляет шифрование данных, используя схему с общим ключом. Данные шифруются быстрым симметричным алгоритмом при помощи ключа шифрования файла FEK (file encryption key). FEK — это случайным образом, сгенерированный ключ определенной длины. Длина ключа в североамериканской версии EFS 128 бит, в международной версии EFS используется уменьшенная длина ключа 40 или 56 бит.

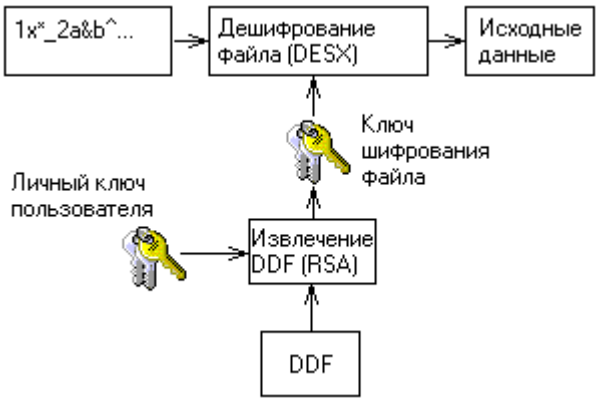
FEK шифруется одним или несколькими общими ключами шифрования, в результате чего получается список зашифрованных ключей FEK. Список зашифрованных ключей FEK хранится в специальном атрибуте EFS, который называется DDF (data decryption field — поле дешифрования данных). Информация, при помощи которой производится шифрование данных, жестко связана с этим файлом. Общие ключи выделяются из пар пользовательских ключей сертификата X509 с дополнительной возможностью использования «File encryption». Личные ключи из этих пар используются при дешифровке данных и FEK. Личная часть ключей хранится либо на смарт-картах, либо в другом надежном месте (например, в памяти, безопасность которой обеспечивается при помощи CryptoAPI).

Процесс шифрования



Незашифрованный файл пользователя шифруется при помощи случайно сгенерированного ключа FEK. Этот ключ записывается вместе с файлом, файл дешифруется при помощи общего ключа пользователя (записанного в DDF), а также при помощи общего ключа агента восстановления (записанного в DRF).

Процесс дешифрования



Сначала используется личный ключ пользователя для дешифрации FEK — для этого используется зашифрованная версия FEK, которая хранится в DDF. Расшифрованный FEK используется для поблочного дешифрования файла. Если в большом файле блоки считываются не последовательно, то дешифруются только считываемые блоки. Файл при этом остается зашифрованным.

Выводы

- Система EFS в Windows предоставляет пользователям возможность зашифровывать каталоги NTFS, используя устойчивую, основанную на общих ключах криптографическую схему, при этом все файлы в закрытых каталогах будут зашифрованы. Шифрование отдельных файлов поддерживается, но не рекомендуется из-за непредсказуемого поведения приложений.
- Система EFS также поддерживает шифрование удаленных файлов, доступ к которым осуществляется как к совместно используемым ресурсам. Если имеют место пользовательские профили для подключения, используются ключи и сертификаты удаленных профилей. В других случаях генерируются локальные профили и используются локальные ключи.
- Система EFS предоставляет установить политику восстановления данных таким образом, что зашифрованные данные могут быть восстановлены при помощи EFS, если это потребуется.
- Политика восстановления данных встроена в общую политику безопасности Windows 2000. Контроль за соблюдением политики восстановления может быть делегирован уполномоченным на это лицам. Для каждого подразделения организации может быть сконфигурирована своя политика восстановления данных.
- Восстановление данных в EFS — закрытая операция. В процессе восстановления расшифровываются данные, но не ключ пользователя, при помощи которого эти данные были зашифрованы.
- Работа с зашифрованными файлами в EFS не требует от пользователя каких-либо специальных действий по шифрованию и дешифрованию данных. Дешифрование и шифрование происходят незаметно для пользователя в процессе считывания и записи данных на диск.
- Система EFS поддерживает резервное копирование и восстановление зашифрованных файлов без их расшифровки. Программа NtBackup поддерживает резервное копирование зашифрованных файлов.
- Система EFS встроена в операционную систему таким образом, что утечка информации через файлы подкачки невозможна, при этом гарантируется, что все создаваемые копии будут зашифрованы
- Предусмотрены многочисленные меры предосторожности для обеспечения безопасности восстановления данных, а также защита от утечки и потери данных в случае фатальных сбоев системы.