ПОДХОДЫ К РЕАЛИЗАЦИИ КОНТРОЛЯ ДОСТУПА К ФАЙЛОВОЙ СИСТЕМЕ В ОС СЕМЕЙСТВА WINDOWS NT

Немкович А.В.

Белорусский государственный университет информатики и радиоэлектроники
г.Минск, Республика Беларусь

Ярмолик В.Н. – д.т.н.,профессор

Целью данной работы является анализ возможных подходов к реализации контроля доступа к файловой системе в операционных системах семейства Windows NT.

На данный момент одной из наиболее важных проблем в области информационных технологиий является проблема защиты и контроля доступа к конфеденциальной информации, к различного вида цифровым данным, хранящимся на компьютерах в виде файлов. В тоже время самыми популярными операционными системами для компьютера среди пользователей являются операционные системы семейства Windows NT, что обуславливает важность изучения подходов к реализации контроля доступа к файловой системе в операционных системах семейства Windows NT.

Прежде чем рассматривать подходы к защите файловой системы с учётом особенностей и возможностей операционных систем Windows NT, необходимо ознакомиться с общепринятыми способами защиты секретной информации, среди которых можно выделить следующие методы:

1) стеганография;

2) криптография.

В случае стеганографии скрывается сам факт сокрытия секретной информации, то есть секретная информация передаётся под видом общедоступной. Наиболее распространенный стеганографический материал — это графические, звуковые и другие мультимедийные данные, формат которых позволяет замещать наименее значимую часть исходной информации на любую произвольную(собственно, на ту самую секретную информацию, которую требуется скрыть) [1].

Метод криптографии основан на прямо противоположном принципе: ни от кого не скрывается факт передачи или хранения секретной информации и не предпринимаются никакие действия для предотвращения доступа к ней посторонних лиц [1]. В большинстве случаев секретные данные шифруются с помощью определенного алгоритма, и, чтобы прочитать их, сначала потребуется их расшифровать, для чего также, скорее всего, необходимо будет знать ключ/ключи, которые использовались для шифрования данных [2].

В данной работе для защиты и контроля доступа к файлам конкретно в операционных системах семейства Windows NT предлагается метод «прозрачного доступа к файлам».

Суть метода «прозрачного доступа к файлу» заключается в том, что файл динамически шифруется при перезаписи/записи его на носитель информации и динамически расшифровывается при его чтении. В операционных системах семейства Windows NT для обеспечения возможности динамического шифрования файла при его записи на диск необходимо разработать свой фильтр-драйвер файловой системы. Фильтр-драйвер – это драйвер, который перехватывает запросы на ввод-вывод (IRPs – Input/Output Request Packets [3]), предназначенные для некоторых существующих программных модулей (например, файловая система или драйвер диска). В зависимости от места вставки в иерархии драйверов фильтр-драйвер будет получать определенные запросы от диспетчера ввода-вывода(I/O Manager [4]) и иметь определенные возможности расширить имеющуюся функциональность, поэтому фильтр-драйвер должен быть вставлен в иерархию драйверов над драйвером каждой файловой системы, чтобы шифровать данные перед тем как послать их файловой системе и дешифровать данные перед тем, как их посылать обратно пользователю. Таким образом, с учётом возможностей, предоставляемых фильтр-драйвером, становится возможным выполнение операций аутентификации и авторизации пользователя системы, а также шифрования данных файлов «на лету», то есть в момент обращения пользователя к файловой системе. При этом сам факт того, что данные файла зашифрованы также может скрываться, поскольку, если пользователь имеет права на доступ к файлу, то файл будет автоматически расшифровываться фильтр-драйвером, которому будет известен ключ шифрования, и пользователь сможет с ним работать так, словно он и не был зашифрован, в ином случае пользователю будет отказано в доступе к файлу.

Список использованных источников:

1. Второе дыхание криптографии [Электронный ресурс] – Режим доступа: https://compress.ru/article.aspx?id=10116 – Дата доступа: 17.03.2019.
2. , С.Г. криптографии / С.Г. , В.В. , Р.Е. Серов. – М: линия – , – – 52 с.
3. Rajeev, N. Windows NT File System Internals: A Developer's Guide / N. Rajeev. – O'Reilly. – 1997. – 774 S.
4. Schrieber, S.B. 2000 : a programmer's cookbook / S.B. Schrieber. – -. – 2001, – 592 S.