УДК 004.4

РАЗРАБОТКА ОБЩЕЙ СТРУКТУРЫ СИСТЕМЫ ЗАЩИТЫ ФАЙЛОВ С ИСПОЛЬЗОВАНИЕМ ФЛЕШ-НАКОПИТЕЛЯ

Шульженко А.А., Братуха М.А., Цололо С.А.
ГВУЗ «Донецкий национальный технический университет», г. Донецк, Украина
gekannt@yandex.ru, astr0n@ukr.net

Аннотация

Шульженко А.А., Братуха М.А., Цололо С.А. Разработка общей структуры системы защиты файлов с использованием флеш-накопителя. *Разработана общая структура и принципы функционирования системы защиты и ограничения доступа с использованием флеш-накопителя. В основе системы лежат криптографические алгоритмы шифрования и многофункциональная база данных, в которой хранятся параметры файлов, информация о флеш-накопителе и ключи доступа. Выполнена реализация и тестирование разработанной системы.*

Введение

Проблема сохранности пользовательских данных в современном информационном пространстве является достаточно актуальной. Причины сокрытия и шифрования данных могут быть различными – от коммерческой тайны и корпоративной этики до сугубо личных пользовательских целей. В общем случае, даже если рабочая станция находится в единоличном использовании, нельзя гарантировать с достаточно степенью надежности, что никто не сможет получить доступ к важной информации.

Обычно пользователь работает с целым набором файлов, который следует оградить от внешнего вмешательства. При этом использование отдельного пароля для каждого файла является нецелесообразным и часто неэффективным из-за человеческого фактора. Поэтому актуальной задачей является разработка универсальной системы управления доступа к файлам посредством мастер-ключа, который позволяет контролировать весь набор зашифрованных файлов. Такой подход значительно упрощает работу пользователю, и повышает уровень защиты пользовательских данных.

1. Общее описание системы защиты файлов

Разработанная система предназначена для защиты и ограничения доступа к пользовательским данным. Использование системы гарантирует сохранность данных и блокировку доступа к ним со стороны пользователей, не имеющим ключа доступа. При этом в качестве ключа используется аппаратно-программная связка флеш-накопителя и пользовательского пароля.

При разработке системы были рассмотрены различные способы защиты, успешно выполняющие поставленные задачи. Одним из таких способов является защита пользовательской информации при помощи флеш-накопителя. Но программы, которые шифруют отдельные файлы и требуют ввода различных паролей для каждого файла, являются уязвимыми как из-за человеческого фактора (забывание, простота паролей), так и из-за использования клавиатурных шпионов. Подобных программ существует достаточно много, при этом многие реализуют это в качестве встроенной функции, например архиватор WinRar.

Основная особенность предлагаемой в данной работе системы заключается в добавлении еще одного уровня защиты. На флеш-накопителе пользователя хранится база данных с ключами, доступ к которой осуществляется по паролю. В целях безопасности база данных хранится зашифрованной. Пользователь выбирает любые файлы в системе и шифрует их, при этом ключи шифрования отдельно для каждого файла генерируется программой автоматически. База данных хранит информацию о флеш-накопителе, поэтому в качестве места хранения самой базы целесообразно использовать этот же флеш-накопитель.

Для дополнительного увеличения уровня стойкости системы к взломам было решено шифровать пользовательские файлы без постоянного мониторинга состояния файлов. Такой подход значительно уменьшает сложность разрабатываемой системы и уменьшает нагрузку на рабочую станцию. Система защиты не находится в режиме постоянного ожидания, а потребляет ресурсы станции только в момент непосредственного взаимодействия с пользователем.

Таким образом, можно выделить следующие задачи, которые выполняет разрабатываемая система:

- Шифрование пользовательских файлов;
- Хранение ключей доступа к зашифрованным файлам на флеш-накопителе в виде базы данных;
- Защита базы данных посредством шифрования и пароля, а так же контроль её целостности;
- Привязка базы данных к флеш-накопителю, на котором она была создана;
- Расшифровка зашифрованных файлов.

2. Разработка структуры системы

Исходя из задач, которые должна выполнять система, была составлена структурная схема взаимодействия компонентов системы (рис. 1).

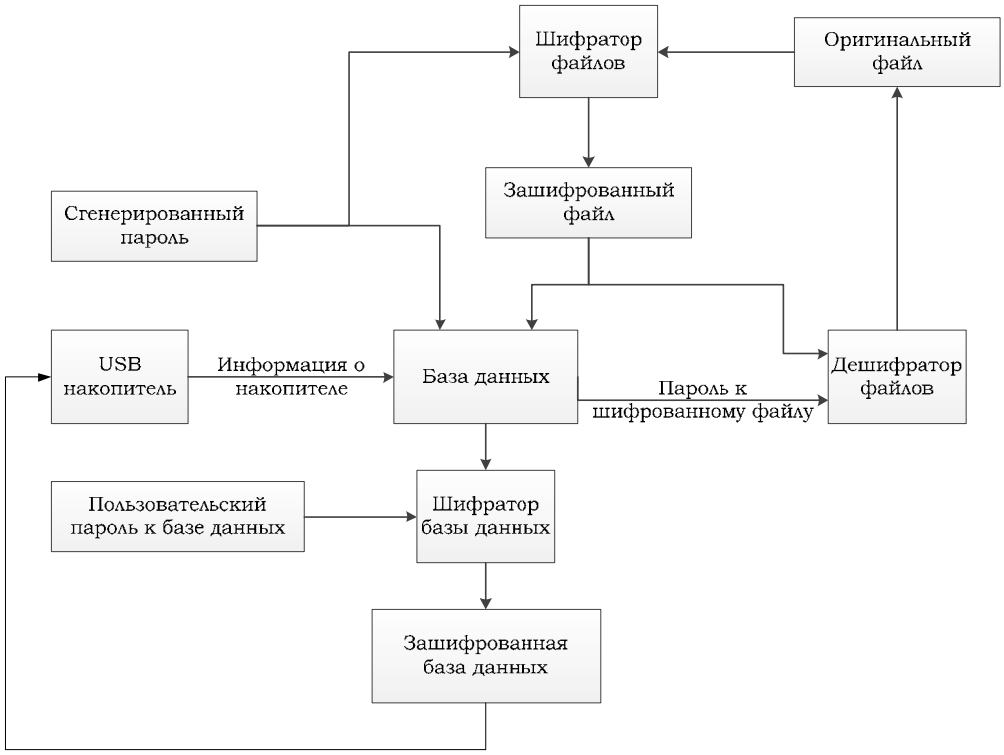

Рисунок 1 – Структурная схема взаимодействия компонентов системы

Далее подробно рассмотрим основные компоненты системы.

Шифратор файлов

На вход шифратора файлов подается поток содержимого файла в бинарном виде и случайный ключ. Шифрование файлов осуществляется с помощью популярного и надежного алгоритма шифрования AES (он же Rijndael) [2], который имеет хорошую криптостойкость. Возможная длина пароля составляет: 128, 196 и 256 бит. Для зашиты была выбрана длина пароля в 128 бит (16 байт) и режим шифрования CBC (Cipher-block chaining), в котором используется вектор инициализации, длинной в 128 бит. Структурная схема данного режима представлен на рис 2.

Алгоритм AES был выбран не только из-за своей высокой криптостойкости и повсеместного использования, даже в госструктурах, но так же из-за того, что этот алгоритм поддерживает аппаратное ускорение на процессорах фирмы Intel, которые стоят на подавляющем большинстве современных рабочих станциях. А это значит, что на них значительно уменьшается время шифрования/расшифровки больших объемов данных.[3]

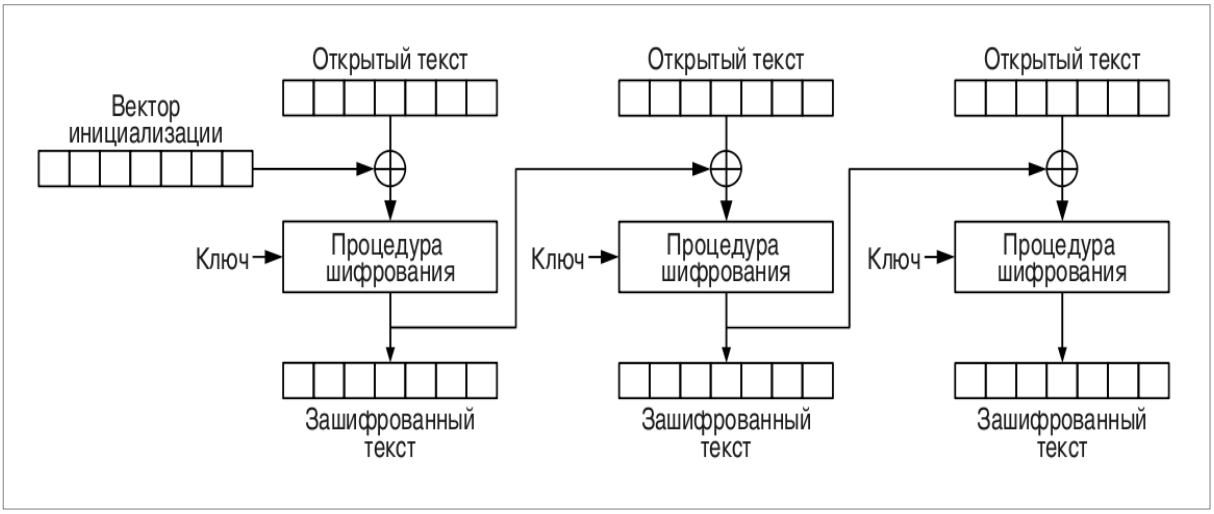

Рисунок 2 – Структурная схема алгоритма шифрования в режиме CBC

Дешифратор файлов

На вход дешифратора подаётся информация о файле из базы данных, зашифрованный файл и ключ доступа к нему. После этого проверяется соответствие поступивших данных и происходит расшифровка, за той же схемой, что и в шифраторе, только наоборот. На выходе дешифратора формируется оригинальный файл.

База данных

База данных является самой важной частью системы защиты. На вход базы данных подается информация о зашифрованном файле, пароль к этому файлу, а так же информация о флеш-накопителе, на котором расположена база данных. Основная ее функция заключается в хранении этих данных в структурированном виде, и подаче на вход дешифратора файлов.

База данных хранится в зашифрованном виде на флеш-накопителе, с которым связана вся система защиты. В виду особенностей библиотеки libusb (для Windows)[5], невозможно получить логическую букву флешки в системе, что влечёт за собой возможность создания базы данных в любом месте компьютера. Данная отрицательная характеристика ложится полностью на плечи конечного пользователя – ведь только от него зависит место, где будет храниться файл базы данных.

Флеш-накопитель

В качестве места хранения базы данных может использоваться любое USB-устройство, способное хранить в себе информация по запросу пользователя. При работе с программой указывается полный путь к накопителю.

Для получения информации о флеш-накопителе используется библиотека libusb [5]. Ввиду особенностей реализации данной библиотеке на системе Windows, прежде чем использовать какой-либо флеш-накопитель для взаимодействия с программой, необходимо установить для него так называемый фильтр (он же драйвер). Этот фильтр устанавливается с помощью специальной утилиты, поставляемой вместе с библиотекой.

Такая особенность вносит некую двойственность в программу. С одной стороны это усложняет использование программы для конечного пользователя, а с другой стороны это увеличивает безопасность всей системы.

3. Структура базы данных

Из рассмотренной структуры системы следует, что в базе данных необходимо хранить информацию о флеш-накопителе для последующей проверки подлинности. Библиотека libusb позволяет получить достаточно много информации о любом USB-устройстве, но лишь несколько полей такой информации способны дать возможность различать устройства. Для разработанной системы были выбраны следующие поля: idVendor (VID), idProduct (PID), Serial Number.

Выбор именно этих полей объясняется следующими причинами:

- Поле VID – это уникальный идентификатор производителя, указывающий на конкретную компанию, которая выкупила его для производства своей линейки USB-устройств. Но для идентификации этого поля недостаточно, так как десятки тысяч различных устройств выпускаются под одним и тем же VID.
- Добавления поля PID – идентификатор устройства вносит более точный отсев. Но и этого недостаточно, так как производителем может быть выпущено множество одинаковых флеш-накопителей, у которых PID будет совпадать.
- Лишь внося поле Serial Number (серийный номер устройства), можно практически полностью быть уверенным в том, что данный накопитель является уникальным.

Конечно же, существует множество способов подменить любое из этих полей, но для разработанной системы это не столь критично, так как даже в случае подмены данных о флеш-накопителе и получении доступа к файлу базы данных еще необходим и пароль для ее открытия. При этом информация о флеш-накопителе хранится в базе данных в виде хеш-суммы [1]. Поэтому даже если рассмотреть базу данных в бинарном виде (когда она расшифрована), то полученные данные не будут нести в себе какой-либо полезной информации.

4. Особенности системы

При рассмотрении какой-либо системы защиты всегда остро стоит вопрос ее надежности и стойкости к взлому. Предлагаемый метод защиты является практически непреодолимым для лиц, желающих узнать содержимое зашифрованных файлов, и не имеющих при этом ничего, кроме этих файлов, особенно в момент, когда программа не запущена и не осуществляет каких-либо действий.

Основными преимуществами разработанной системы являются:

- Небольшое потребление ресурсов рабочей станции;
- Высокий уровень защиты файлов;
- Переносимость и легковесность.

Недостатком разработанной системы является возможность перехватить данные, если система активна и взаимодействует с базой данных. При шифровании/расшифровке базы данных используются потоки, которые можно успешно перехватить и перенаправить путем манипуляций с дизассемблированным кодом. Также необходимо отметить, что при получении доступа к флеш-накопителю база данных может быть взломана. Для этого могут применяться различные способы, например, простой перебор (brute force). Данный способ взлома очень эффективен, особенно если пользователь использовал пароль не более шести символов. В таком случае база может быть взломана достаточно быстро на рабочей станции со средней производительностью. Однако этот недостаток связан исключительно с особенностями человеческого фактора и не может быть полностью исключен.

Выводы

В данной работе был рассмотрен один из методов защиты данных – с помощью шифрования и привязке к флеш-накопителю. Метод защиты путем привязки к какому-либо устройству является достаточно популярным, практичным и используется повсеместно. Например, некоторые компании используют его для защиты своих программных продуктов. Популярность метода объясняется еще и тем, что от конечного пользователя требуется лишь наличие нужного флеш-накопителя.

В данной работе предлагается система, которая объединяет аппаратный и программный подходы к защите пользовательских данных. Это позволяет обеспечить более высокий уровень защиты пользовательских данных по сравнению с известными полностью программными решениями.

Список литературы

1. Bruce Schneier Applied Cryptography Second Editio. – John Wiley & Sons, 1996 Paperback – 784 p. , chapter 18
2. Michael Welschenbach Cryptography in C and C++ translated by David Kramer. –
3. 2nd American ed., rev. and enl, 2005 – 422 p. - p.279
4. Нильс Фергюсон, Брюс Шнайер, Практическая криптография. : Пер. с англ. – М.: Издательский дом «Вильямс», 2005 – 424 с.
5. Документация по криптографической библиотеке Botan [электронный ресурс]. – Режим доступа: http://botan.randombit.net/.
6. Документация по библиотеки для работы с USB-устройствами [электронный ресурс]. – Режим доступа: http://www.libusb.org/.
7. Документация по криптографической библиотеке Crypro++ [электронный ресурс]. – Режим доступа: http://www.cryptopp.com/