Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.457

Черник
Константин Юрьевич

Модели и средства криптографической защиты данных на мобильных носителях информации

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В. Н.
д.т.н., профессор

Минск 2015

Библиотека БГУИР

ВВЕДЕНИЕ

Хищения данных превратились сегодня в одну из наиболее серьезных угроз для информационной безопасности. Ежегодные отчёты крупнейших компаний мира показывают, что масштабы проблемы колоссальны. Так по данным ФБР в США в 2014 г. на 100 тыс. населения приходилось от 44 до 667 жалоб на кибер-преступления либо мошенничество. В 2013 году система IDS, входящая в состав Kaspersky Internet Security, отразила 219 899 678 сетевых атак. Аналогичный показатель 2008 года составил чуть более 30 млн. инцидентов.

Даже небольшие утечки могут подорвать доверие, нанести финансовый урон или просто разорить компанию. В связи с этим защите данных на мобильных носителях информации уделяется особое внимание, так как именно эта категория носителей наиболее подвержена утечкам (утеря, кража). Большинство существующих моделей защиты данных на мобильных носителях информации содержат серьёзные недостатки, которые ставят под сомнение надёжность этих подходов.

В данной работе мы проведём анализ существующих моделей защиты данных на мобильных носителях информации, постараемся выявить плюсы и минусы текущих решений. Основываясь на результатах анализа, мы разработаем требования к оптимальной модели защиты данных на мобильных носителях информации и спроектируем эту модель. Так же мы разработаем прототип программного средства УХИ, в основу которого ляжет разработанная нами, наиболее оптимальная модель защиты данных. Данная реализация позволит нам доказать техническую возможность реализации разработанной модели защиты. Кроме того, реализованное программное средство может быть использовано в качестве готового решения для эффективной защиты данных на мобильных носителях данных.

В дополнение мы проведём анализ технологий, которые будут использованы при создании программного средства. Выбор технологий так же будет осуществлять с учётом особенностей разработанной модели и будет направлен на получение наиболее эффективного решения.

В результате прототип УХИ будет основываться на самой современной и эффективной модели защиты, что позволит безопасно использовать это средство для надёжной защиты данных на мобильных носителях. Разработанное решение будет полностью соответствовать законодательству Республики Беларусь, что позволит сертифицировать его и использовать в сферах, требующих самый высокий уровень секретности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Библиотека БГУИР

Цель и задачи исследования

Целью данного исследования является разработка модели и программного средства хранения информации в защищенном путем шифрования виде на мобильных носителях информации.

Для достижения намеченной цели были сформулированы следующие задачи:

- Изучить существующие модели криптографической защиты данных, способы атак на защищаемые данные;
- Провести анализ современных моделей защиты данных на USB носителях информации;
- Основываясь на результатах анализа разработать наиболее эффективную модель защиты данных, которая будет положена в основу прототипа УХИ.
- Создать программное обеспечение в соответствии с разработанной спецификацией и архитектурой;
- Произвести тестирование функциональных возможностей прототипа и определить его эксплуатационные ограничения.

Объектом данного исследования являются модели защиты данных на мобильных носителях информации, а так же прототип, в основу которой положена наиболее эффективная модель защиты.

Предметом исследования являются методы и алгоритмы криптографической защиты данных.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы тесно связана со студенческой научной работой, выполненной на первом уровне образования "Криптографическое средство защиты данных на мобильных носителях информации". Отдельные части диссертации подготовлены в связи с выполнением задач для предприятия НТЦ "Контакт", поставленных в связи с разработкой коммерческого продукта УХИ "Меркурий" (ГБ № 11-2004, № ГР 20111065).

Тема диссертационной работы соответствует приоритетным направлениям фундаментальных и прикладных научных исследований Республики Беларусь, утвержденных Постановлением Совета Министров Республики Беларусь № 585 от 19.04.2010 г. (5.5. методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы).

Личный вклад соискателя

Библиотека БГУИР

Диссертационная работа отражает личный вклад соискателя в исследования, выполненные в БГУиР в период обучения в магистратуре. Основные результаты диссертации, получены лично соискателем.

Постановка задач, математические модели и обсуждение результатов проводились с научным руководителем. Алгоритмы разработаны соискателем самостоятельно.

Проектирование и разработка программного обеспечения выполнены автором самостоятельно.

Апробация результатов диссертации

Основные результаты диссертационной работы докладывались и обсуждались на международной конференции

Опубликованность результатов диссертации

Результаты диссертационной работы опубликованы в 1 статье в сборнике материалов и трудов научных конференций.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка. Общий объем диссертации составляет 109 с., включая 27 рисунков, 30 библиографических ссылок.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приведен краткий исторический очерк, определено место проблемы защиты данных в современном мире, приведена общая оценка современного состояния исследований и разработок в данной области. Определено место текущего исследования в области защиты данных на мобильных носителях информации.

В первой главе представлен анализ литературных данных по криптографической защите информации. Проведен анализ существующих методов шифрования, подробно рассмотрены особенности алгоритмов симметричного шифрования: использование только одного ключа, который используется и при шифровке, и при расшифровке. Симметричное шифрование не отличается большой стойкостью против взлома, зато процесс кодировки/раскодировки происходит очень быстро.

При ассиметричном шифровании создается два ключа – открытый и закрытый. Открытый ключ используется при шифровке, поэтому особой секретности не представляет. Закрытый (или приватный) ключ используется

Библиотека БГУИР

при расшифровке, поэтому тщательно хранится. Такая система более устойчива ко взлому, но процесс шифрования может занимать заметное время. Поэтому часто используют комбинированный способ – все данные шифруются симметричным алгоритмом, а в конце скрепляются шифром с открытым ключом.

Для обеспечения безопасности хранящихся данных целесообразно использовать симметричный алгоритм шифрования по нескольким причинам: пользователь у флешки будет только один, а значит никаких обменов ключами и зашифрованной информацией со сторонними лицами не предусматривается. Так как шифрование и расшифрование будет происходить во время чтения и записи на диск, критичным является скорость выполнения операций.

Симметричные алгоритмы шифрования бывают двух видов: потоковые алгоритмы, а также блочные шифры. Алгоритмы блочного шифрования используют для работы наборы данных фиксированной длины, т.е. шифруемое сообщение разбивается на блоки, последовательно обрабатываемые алгоритмом. Результатом обработки одного блока текста является шифрооблок того же размера. Так как нам придётся шифровать блоки из различных частей диска, мы не можем использовать шифры поточного шифрования, а так же блочные с эмитовставками. Таким образом, для наших целей подходит только алгоритм блочного шифрования. Наиболее известны алгоритмы блочного шифрования DES, 3DES и AES . В Республике Беларусь в качестве стандарта принят алгоритм блочного шифрования ГОСТ 28147-89. Он был выбран как наиболее подходящий по нескольким причинам:

1. Не уступает по стойкости ни одному из рассмотренных выше алгоритмов шифрования.
2. Не уступает по скорости, что является критичным фактором в проектируемой системе.
3. Является официально используемым стандартом на территории РБ, что позволяет доверять этому алгоритму.
4. Является совместимым со всем программным обеспечением, выпускаемым на территории РБ, что позволит в будущем расширять функциональность данной системы. Кроме того, на основе данного алгоритма построен отечественный стандарт хеширования ГОСТ Р 34.11-94.

Во второй главе описаны существующие модели защиты данных на USB носителях информации.

Модель-1: запаковать данные в архив с паролем.

Модель-2: программное шифрование данных - и программ для этого множество, как платных, так и бесплатных, например, TrueCrypt. Однако,

Библиотека БГУИР

возникают некоторые проблемы с переносимостью данных и обеспечением компьютеро-независмости при их использовании. Еще один недостаток - нужно не забывать перед выниманием флешки размонтировать раздел.

Модель-3: аппаратное шифрование данных средствами контроллера самой флешки, например, Kingston DataTraveler Secure с шифрованием AES-256. Данный способ с точки зрения информационной безопасности аналогичен предыдущему способу, но полностью не зависит от компьютера и учетной записи пользователя - единственное, что требуется - это открыть закрытый раздел путем ввода пароля. Соответственно, для указанных целей производитель флешки предлагает специальную программу для разбивки общего объема на открытую и секретную части, изменения пароля и т.п. Недостаток - разновидностей таких флешек немного, да и стоимость относительно высока.

Модель-4: шифрование данных на флешке отсутствует, но раздел на флешке может быть закрыт паролем средствами контроллера самой флешки.

Аппаратное шифрование возможно только на специальных накопителях. Например, на всех U3-совместимых накопителях. Установив на такую флешку пароль, пользователь лишает злоумышленников всяких шансов увидеть секретную информацию. Специальный криптографический чип во флешке обеспечивает аппаратное шифрование данных. Дополнительно, на небольшой загрузочной области флешки имеется специальная программа, отвечающая за работу шифровальных функций. Пока пользователь не введет пароль, основной раздел для него закрыт.

В третьей главе описана подробная спецификация требований, предъявляемых к наиболее эффективной модели защиты данных на мобильных носителях информации. Определены основные функциональные возможности модели:

– аутентификация субъектов, зарегистрированных в УХИ по паролю;
– смена ключевой информации в случае компрометации ключей;
– защита целостности информации путем помещения ее в область предназначенную только для чтения;
– обеспечение конфиденциальности данных пользователя путем шифрования по ГОСТ 28147-89 в области доступной для чтения и записи;
– контроль целостности и периодическое тестирование УХИ средств обеспечения безопасности;
– хранение ключей пользователя вне файловой системы (16 областей по 64кБайт) с организацией доступа к ним через специальный программный интерфейс;

Библиотека БГУИР

– ведение журнала действий пользователя;

– введение ограничения на выполнение программы при использовании УХИ;

– экстренное уничтожение хранимой информации.

На основе описанных требований разработана архитектура программного средства.

Программное средство должно предоставлять возможность оперировать критическими объектами операционной системы в режиме ограниченных прав пользователя. А так же встраиваться в систему, для того что бы процесс чтения и записи с шифруемого устройства не отличалась с точки зрения пользователя от обычного носителя информации. Это порождает некоторые ограничения, накладываемые на архитектуру данного программного средства:

– Часть системы должна быть оформлена в виде драйвера.

– Должен быть интерфейс пользователя для взаимодействия с драйвером

– Должна быть динамическая библиотека (dll) для взаимодействия сторонних программ с драйвером (API системы)

Основная функциональная нагрузка будет лежать на драйвере, так как на уровне ядра мы обладаем практически неограниченными правами в операционных системах семейства Windows.

Данная архитектура позволяет использовать сборки системы в рамках других систем без перекомпиляции их исходных кодов. Также система позволяет добавлять функциональность приложения путем подключения дополнительных модулей также без перекомпиляции существующих сборок системы.

На основе разработанной архитектуры программного средства осуществлено детальное проектирование системы.

Разработанная модель является результатом анализа существующих моделей защиты данных на мобильных носителях информации и включает в себя подробную спецификацию, которая может быть легко положена в основу программного обеспечения, предназначенного для защиты данных на usb накопителях. Кроме того, модель архитектуры предполагает проектирование расширяемой архитектуры программного средства.

В четвёртой главе разработан прототип устройства: программного средства хранения информации на мобильном носителе информации в защищенном путем шифрования по ГОСТ 28147-89 виде. Расшифрование информации производится после считывания зашифрованной информации в память ПЭВМ. Зашифрование информации производится перед записью

Библиотека БГУИР

открытой информации на флеш-диск. Ключи шифрования вырабатываются из пароля введенного пользователем и константы, хранящейся в секторе 1 диска.

В УХИ реализованы следующие криптографические алгоритмы:

– Алгоритмы шифрования. Реализован алгоритм установки защиты (зашифрование) и алгоритм снятия защиты (расшифрование). Алгоритмы предназначены для защиты информации хранящейся в УХИ.

– Алгоритм хэширования. Предназначен для вычисления контрольных характеристик системных объектов. Используется при генерации ключа пользователя.

– Генерация ключей и параметров. Не имеют долговременных параметров.

– Ключ вырабатывается с помощью вычисления значения хэш-функции от пароля, вводимого оператором и выполнения операции XOR с константой, хранящейся в 1-м секторе флеш-диска. Ключ записывается в ОЗУ ПЭВМ и хранится в течение сеанса. По завершении сеанса ключ уничтожается. Ключ уничтожается также при извлечении УХИ из разъема ПЭВМ.

– Контроль времени выполнения. Алгоритмы шифрования относятся к классу симметричных. Время их выполнения не зависит от значений ключей.

Алгоритм хеширования является бесключевым. При хешировании объектов, которые могут оказаться критическими, время хеширования не зависит от значения объекта и определяется только размером объекта.

Клиентская программа представляет собой программный модуль, написанный на языке C++ с использованием прямых вызовов WIN API. Включает в себя графический интерфейс пользователя и внутреннюю логику взаимодействия с драйвером системы. Его задача заключается в владением объектом ядра- драйвером, и выполнением, в соответствии с действиями пользователя, запросов к драйверу. Запросы выполняются с помощью WIN API функции DeviceIOControl. Содержит набор классов для работы с журналом, настройками политик безопасности, а так же класс для инкапсуляции функций графического интерфейса. Наиболее важным функциональным блоком является модуль загрузки драйвера, который проверяет, установлен ли драйвер в системе, и, если драйвер отсутствует, устанавливает его при помощи SCM менеджера.

В пятой главе произведено тестирование реализованной модели защиты данных. Результаты тестирования подтверждают работоспособность разработанного программного средства и корректность реализованных

Библиотека БГУИР

функций, а так же подтверждают техническую возможность реализации требований, предъявляемых к наиболее эффективной модели защиты данных на мобильных носителях информации.

Проверка качества защиты (обеспечения конфиденциальности) программ и данных путем шифрования проводится посредством проверки программных модулей, реализующих криптографические алгоритмы на соответствие ГОСТ 28147-89, на наличие сертификата соответствия и корректности вызовов встраивания криптографических модулей путем исследования исходных текстов программ и анализом всех точек вызова на корректность.

Для работы всех компонентов функционирующих с УХИ, необходимо выполнение следующих условий:

Совместимая ПЭВМ, работающая под управлением ОС семейства MS Windows 2000/XP/2003/Vista/7; наличие свободного разъема USB на ПЭВМ.

Для работы с УХИ пользователь должен быть зарегистрирован в УХИ, для чего ему необходимо определить: пароль и возможность его смены (при необходимости);

Для эксплуатации и эффективного применения УХИ, поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов требуется соблюдение правил хранения УХИ, а также учет носителей информации.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В диссертации проведен анализ существующих методов криптографической защиты данных, атак на защищаемые данные, произведено сравнение различных существующих решений в этой области. Выявлены их сильные и слабые стороны.

Рассмотрены основные модели защиты данных на мобильных носителях информации. На основе анализа существующих моделей разработана подробная спецификация требований к оптимальной модели защиты данных на мобильных носителях информации. В спецификации подробно описаны все функциональные возможности, которыми должен обладать создаваемый программный продукт.

Описаны математические модели, необходимые для создания программного средства. Определены основные направления развития этой области. Так же разработана архитектура программного средства, взаимодействие различных модулей в рамках разрабатываемой системы программного обеспечения. Выбраны средства разработки: язык, IDE, целевая операционная система, дополнительные программы, необходимые для разработки.

Непосредственно разработан прототип программного средства, детально описан процесс создания каждого модуля системы. Приведены наиболее важные фрагменты кода для наглядного понимания процесса реализации проекта. Создана программная инфраструктура: контроллер (драйвер), пользовательский интерфейс (клиентская программа), API системы (динамически загружаемая библиотека).

Произведено тестирование разрабатываемых программных модулей прототипа, детально расписан процесс проверки различных функциональных возможностей системы программных модулей.

Детально описан процесс взаимодействия пользователя с программным продуктом. Составлена подробная инструкция по эксплуатации. Приведены различные примеры использования и различные виды нестандартного поведения (ошибок) взаимодействия пользователя с программным средством.

Данный прототип фактически является полноценным средством защиты данных на мобильных носителях информации, реализующий базовую функциональность. Прототип программного средства позволяет сократить расходы на обеспечение безопасности информации, а именно, избавиться от технических средств обеспечения безопасности (сейфы, электронные замки), сократить время взаимодействия человека с компьютером для обеспечения безопасности информации, что частично

Библиотека БГУИР

освободит рабочее время, кроме того, применение журнала значительно упрощает работу следственных органов в случае возникновения прецедента.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 – Yarmolik, V. FEATURES OF DATA PROTECTION COMPLEX "MERCURY" FOR USB MEMORY STICK / Yarmolik V., Chernik K. // The Youth of the 21st Century: Education, Science, Innovations : materials of the International Conference for Students, Postgraduates and Young Scientists; Vitebsk, December 4, 2014 / Vitebsk State University; Editorial board.: I.M. Prischepa (editor in chief.) [and others.]. – Vitebsk : VSU named after P.M. Masherov, 2014. –p. 37.

Библиотека БГУИР