ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Л.К. Бабенко, А.Ю. Коробко, О.Б. Макаревич, О.Ю. Пескова
Россия, г.Таганрог, ТРТУ

ОПЫТ РАЗРАБОТКИ СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ ОС МСВС 3.0

Введение

В настоящее время существует несколько дистрибутивов операционной системы (ОС) Linux от российских производителей (ASP Linux, ALT Linux, МСВС). Наиболее защищенным из них является ОС МСВС 3.0.

Эта операционная система имеет свои неоспоримые достоинства, в частности, отметим поддержку мандатного разграничения доступа к ресурсам системы и другие системные средства защиты информации. Но можно выделить и довольно существенные недостатки: достаточно старая версия ядра, взятого за основу в МСВС, не поддерживает некоторое аппаратное обеспечение, ставшее стандартным в современных компьютерах (например, USB), слабо представлены и криптографические средства. В ОС МСВС имеется утилита шифрования файлов, которую пользователь должен запускать до и после сеанса работы с файлом, подлежащим защите. Однако такая схема имеет очевидные недостатки – во время использования файл тоже остается открытым, а кроме того, пользователь может по разным причинам (либо случайно, либо преднамеренно, либо в результате технического сбоя) не зашифровать файл после работы с ним. В этом случае злоумышленник может получить доступ к секретным данным, что недопустимо. Поэтому перед авторским коллективом была поставлена задача – создание комплекса дополнительных аппаратно-программных средств, позволяющих повысить уровень основных подсистем защиты от несанкционированного доступа (НСД). Были реализованы следующие средства повышения защищенности ОС МСВС 3.0.

1. Реализация схем аутентификации (идентификации) пользователя с использованием РИК и eToken RIC. Данная программная компонента реализована в виде системной библиотеки и может использоваться как вместе с разработанным подключаемым модулем аутентификации (PAM), так и при создании новых программных средств, реализующих механизмы защиты от НСД. Модуль PAM предназначен для аутентификации пользователя в приложениях, использующих сервис PAM, путем предъявления секретного ключа, расположенного на защищенном носителе РИК или eToken RIC. При разработке новых приложений можно использовать библиотечные вызовы библиотеки РИК для доступа к ключевой информации, размещенной на РИК и eToken RIC.

2. Реализация механизмов и процедур взаимной аутентификации пользователей, вступающих в информационный обмен по сетям связи. Эта подсистема реализована в виде программной библиотеки, используемой приложениями пользователей, вступающих в информационный обмен по сетям связи. При этом ключи аутентификации хранятся в центре сертификации. Используемые криптографические алгоритмы соответствуют ГОСТ (исключение составляет алгоритм RSA, так как не существует отечественного стандарта для несимметричных алгоритмов шифрования данных).

3. Реализация защищенной передачи данных. Данная программная компонента выполнена в виде модуля ядра и реализует функции прозрачного шифрования данных на канальном уровне, для чего использован протокол IPSec, функциони-

рующий в режиме ESP. Это позволяет осуществлять прозрачное шифрование передаваемых и получаемых по сети данных с использованием алгоритма симметричного шифрования ГОСТ 28147-89, а также осуществляется защита от подмены сообщений и другие функции. Для работы с модулем необходимо указывать адреса вычислительных систем, обмен данными с которыми должен осуществляться с использованием прозрачного шифрования. Таким образом, организуются виртуальные частные сети.

4. Реализация программной компоненты, осуществляющей прозрачное шифрование части файловой системы. Данная подсистема реализована в виде модуля ядра и осуществляет шифрование файлов, заданных префиксом имени файла, по алгоритму симметричного шифрования ГОСТ 28147-89.

5. Реализация программной части, осуществляющей проверку целостности программной среды рабочей станции на этапе загрузки системы. Данная компонента осуществляет вычисление циклических контрольных сумм файлов, заданных списком. Модуль реализован на языке ассемблера и не использует функций BIOS и ОС. Таким образом, он может быть встроен в виде прошивки ПЗУ в «электронный замок» НТЦ Атлас.

6. Реализация программного обеспечения центра сертификации, демона операционной системы и библиотек, используемых прикладными программами. Также реализуется утилита администрирования с графическим пользовательским интерфейсом для добавления новых пользователей в базу данных и настройки центра сертификации. В качестве хранилища сертификатов используется СУБД MySQL. Система реализует стандарт X.509.

7. Реализация утилиты администрирования доступом к ресурсам рабочих станций на основе мандатного и дискреционного доступа.

8. Реализация подсистемы регистрации и аудита. Данная подсистема состоит из демона аудита, собирающего информацию по специальному протоколу, и утилиты с графическим пользовательским интерфейсом для просмотра и поиска необходимой информации.

9. Реализация программного обеспечения для текстонезависимой аутентификации пользователя «по голосу». Программная подсистема реализуется в виде нескольких компонент: утилита администрирования и подключаемый модуль аутентификации. Разработанная подсистема позволит использовать биометрические данные пользователя (в частности голос) в виде параметров аутентификации. Использование PAM позволяет использовать разработанную подсистему в ряде приложений, ее поддерживающих.

Рассмотрим более подробно реализацию криптографической подсистемы и подсистемы аутентификации и разграничения доступа.

Криптографическая подсистема

Задача обеспечения конфиденциальности данных и программного обеспечения, расположенных на внешних запоминающих устройствах, решается путем использования алгоритмов криптографических преобразований. При этом целесообразно использовать симметричные криптографические алгоритмы, так как нет необходимости в разделении исполнителей функций шифрования и расшифрования.

Для повышения уровня защищенности операционной системы с помощью средств криптографии необходимо было разработать ряд методов и на их основе реализовать соответствующие программные средства: прозрачного шифрования файловой системы; канального шифрования сетевого трафика; инфраструктуры открытых ключей. Первые две подсистемы построены как модули ядра, что позволяет добиться максимального уровня защищенности и обязательности использования пользователем и прикладным программным обеспечением. Только системный

администратор имеет надлежащие полномочия для управления подсистемами защиты от НСД. Прозрачное шифрование файловой системы снимает указанные выше недостатки средств шифрования, работающих только в режиме диалога с пользователем. Основными достоинствами прозрачного шифрования файлов являются:

- прозрачность для программного обеспечения, что снимает необходимость его модификации;
- прозрачность для пользователя, что позволяет исключить человеческий фактор в вопросе зашифрования/расшифрования информации, поскольку эти операции будут производиться в автоматическом режиме при разрешенных запросах на чтение и запись данных;
- хранение открытых данных только в оперативной памяти ядра, что, в частности, исключает возможность появления защищаемых данных в открытом виде на диске после аварийного завершения работы ОС.

Для обеспечения шифрования данных, хранимых на диске в ОС МСВС, необходимо было реализовать модуль операционной системы, в задачи которого входит:

- прозрачное шифрование данных хранимых в файлах на диске по алгоритму ГОСТ 28147-89;
- обеспечение интерфейса управления на уровне ядра для ввода нового ключа шифрования;
- обеспечение интерфейса управления на прикладном уровне для ввода нового ключа шифрования, а также для обеспечения вспомогательных операций.

Дополнительно разработаны следующие утилиты: генерации нового ключа шифрования; управления модулем.

Реализация подсистемы прозрачного файлового шифрования в виде модуля позволила повысить защищенность системы в целом, так как данные и подпрограммы, принадлежащие модулю, недоступны на прикладном уровне. Функционирование модуля обеспечивается механизмом перехвата системных вызовов операционной системы. Вместо соответствующих процедур ОС управление получает код модуля, который по завершении необходимых действий вызывает первоначальные процедуры ядра.

Использование модуля прозрачного шифрования файловой системы с целью защиты информации от НСД, размещенной на внешних носителях, позволяет унифицировать процесс шифрования, тем самым достигается прозрачность интерфейса для прикладных программ, работающих с файлами, а также индифферентность по отношению к действиям пользователей. Это означает, что пользователь не может обойти систему прозрачного шифрования или отключить ее. Ему доступны только функции по смене ключа шифрования. Таким образом, каждый пользователь имеет собственный ключ шифрования, и файлы, зашифрованные каким-либо ключом, не могут быть расшифрованы другим ключом.

При наличии исходных текстов ядра операционной системы МСВС может быть реализовано множество вариантов выбора файлов для шифрования, например шифрование файлов, расположенных в одной директории (ядро МСВС было модифицировано таким образом, что структуры данных, используемые для управления файлами, инициализированы в NULL). Также при наличии исходных текстов ядра ОС МСВС можно достичь увеличения производительности по времени, за счет добавления промежуточных буферов данных, что позволит отказаться от использования функций доступа к памяти прикладного уровня. Для операции записи блока данных увеличение производительности может достигнуть примерно 1,5 – 2 раза, а для операции чтения – 1,3 раза. Таким образом, прозрачное шифро-

вание файловой системы осуществляется по российскому алгоритму симметричного шифрования ГОСТ 28147-89 в режиме гаммирования с обратной связью. При этом каждый пользователь в начале сеанса работы должен предъявить соответствующий ключ, который может располагаться на дискете, смарт-карте, электронном брелке и т.п. Для того, чтобы это стало возможным, в данной работе было разработано специальное программное обеспечение для работы с российскими интеллектуальными картами РИК и брелками
e-token, в частности, библиотеки работы с этими устройствами, драйвера для работы с USB и т.д.

К достоинствам данной реализации подсистемы прозрачного шифрования следует отнести следующие параметры:

- защита модуля от действий пользователя (например, пользователь не может отключить систему прозрачного шифрования; эта функция доступна только системному администратору);
- использование отечественного стандарта шифрования;
- возможность работы с различными ключами;
- возможность шифрования отдельных файлов, в то время как остальные файлы будут расшифрованы.

Недостатками являются снижение производительности при доступе к файлам за счет введения дополнительных вычислительных алгоритмов, невозможность поддержки функции отображения файла в память для шифруемых файлов. Данные недостатки могут быть устранены при условии наличия исходных кодов ядра операционной системы МСВС 3.0.

Для защиты данных, передаваемых по каналам связи, могут применяться различные методы построения защищенных виртуальных сетей.

Для защиты ОС МСВС 3.0 было принято решения использовать протокол IPSec в режиме туннелирования. Это обосновывается наибольшей распространенностью данного протокола, а также его высокой надежностью. Организация защищенной передачи данных заключается в создании ассоциации безопасности (АБ), которая содержит параметры шифрования и IP-адреса вычислительных систем. Все АБ содержатся в специальной базе данных. Таким образом, используя АБ, можно организовать защищенный обмен данными как в пределах всей сети, так и в отдельном ее сегменте. Помимо того, существует возможность создания виртуальных частных сетей, позволяющих объединять локальные сети через общедоступные каналы связи.

Доработка ОС МСВС 3.0 путем реализации протокола IPSec позволяет повысить уровень защищенности рабочей станции компьютерной сети, путем шифрования передаваемой информации по незащищенным каналам связи. При этом в отличие от стандарта IPSec в качестве алгоритма шифрования используется отечественный стандарт ГОСТ 28147-89. Таким образом, канальное шифрование призвано защитить передаваемую по сетям связи информацию от перехвата. Это достигается путем шифрования данных отправителем и расшифрования получателем. При этом, как и в случае с прозрачным файловым шифрованием, весь процесс происходит прозрачно и для пользователя, и для программного обеспечения на обеих сторонах звена связи. Данная программная компонента выполнена в виде модуля ядра и реализует функции прозрачного шифрования данных на канальном уровне. Для работы с модулем необходимо указывать адреса вычислительных систем, обмен данными с которыми должен осуществляться с использованием прозрачного шифрования. Кроме криптографической защиты сетевого трафика, обеспечивающей защиту конфиденциальности данных, предлагаемый подход предоставляет возможность организовать взаимную аутентификацию взаимодействую-

щих сторон, а также защиту целостности и подлинности передаваемой информации.

К достоинствам предлагаемого подхода можно отнести следующие его возможности:

1. Инкапсуляция многопротокольного не маршрутизируемого трафика в один маршрутизируемый протокол.

2. Защита подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;

3. Защита информации в процессе передачи по открытым каналам связи.

4. Аутентификация взаимодействующих сторон.

5. Криптографическое закрытие передаваемых данных.

6. Подтверждение подлинности и целостности доставленной информации.

7. Защита от повтора, задержки и удаления сообщений.

8. Защита от отрицания фактов отправления и приема сообщений.

9. Организация виртуальных частных сетей через публичные незащищенные сети типа Internet.

К недостаткам же относятся:

1. Необходимость настройки рабочих станций, входящих в виртуальную частную сеть.

2. Необходимость предварительного обмена симметричными ключами шифрования.

3. Снижение производительности вычислительной системы и, как следствие, пропускной способности канала.

Для полноценной работы разработанных подсистем криптографической защиты данных и аутентификации необходимо было создать средства генерации, распределения и хранения ключевой информации.

Программный комплекс инфраструктуры открытых ключей (ИОК) позволяет организовать защищенное хранилище сертификатов и последующее их использование в распределенных системах и сетях передачи данных.

ИОК базируется на стандарте X.509 и состоит из центра сертификации, реализованного в виде демона, центра регистрации, реализованного в виде набора программ, предназначенных для создания сертификатов конечных пользователей и задания основных параметров системы взаимной аутентификации, и конечного пользователя, реализованного как набор библиотечных вызовов, посредством которых программы могут использовать ИОК; имеются функции запроса сертификата, запроса имени владельца сертификата и т.д.

Центр сертификации является основной управляющей компонентой ИОК и выполняет рассылку сертификатов в ответ на запросы пользователей, причем сертификаты снабжены цифровой подписью, что гарантирует их неизменность и достоверность того, что отправителем является центр сертификации.

Центр регистрации - управляющая компонента ИОК, предназначенная для регистрации конечных пользователей. Основная задача ЦР - регистрация пользователей и обеспечение их взаимодействия с ЦС.

Информация о пользователях и их открытые ключи хранятся в специальной базе данных - хранилище сертификатов, в качестве которого используется одна из СУБД на выбор пользователя: MySQL (одна из самых производительных систем) или ЛИНТЕР (российская СУБД с повышенным уровнем защищенности от НСД). К хранилищу сертификатов обращается Центр сертификации с запросом на поиск сертификата заданного пользователя. Центр регистрации производит добавление и удаление пользователей и сертификатов.

В разработанный программный комплекс также входит библиотека взаимной аутентификации пользователей, вступающих в информационный обмен по сетям связи, которая построена на базе стандарта X.509 с использованием отечественных алгоритмов симметричного шифрования и генерации электронной цифровой подписи (ЭЦП): алгоритм криптографического преобразования ГОСТ 28147-89; функция хэширования ГОСТ Р 34.11-94; процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма, описанного в российском стандарте по ЭЦП; алгоритм несимметричного шифрования RSA. Проверка целостности хранимой и передаваемой по сетям связи информации также реализована на основе ЭЦП. Для проверки целостности программной среды был разработан модуль, реализующий метод проверки целостности на основе контрольных сумм, который предназначен для встраивания в качестве прошивки ПЗУ в электронный замок НТЦ «Атлас», что позволит доработать его до уровня аппаратно-программного модуля доверенной загрузки. Модуль реализован на языке ассемблера и не использует функций BIOS и ОС.

Подсистема аутентификации и разграничения доступа

Методы аутентификации субъекта подразумевают обмен аутентификационной информацией, имеющий своей целью убедить верификатора в подлинности идентификатора, предъявленного претендентом. В данной работе реализована система взаимной аутентификации субъектов с отрытым ключом, основанная на стандарте CCITT Recommendation X.509 и следующих криптографических алгоритмах: алгоритм криптографического преобразования ГОСТ 28147-89; функция хэширования ГОСТ Р 34.11-94; процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма ГОСТ Р 34.10-94; алгоритм несимметричного шифрования RSA

В целом, система взаимной аутентификации, построенная на базе стандарта X.509 с использованием отечественных алгоритмов симметричного шифрования и генерации ЭЦП, гарантирует достоверность взаимной аутентификации, но, в виду вычислительной сложности использованных в данной реализации криптографических алгоритмов, обладает не очень высоким быстродействием.

Подсистема разграничения доступа базируется на системе PAM (Pluggable Authentication Modules - Подключаемые модули аутентификации).

Гибкость PAM в этом случае заключается в том, что системный администратор может менять протокол и схемы аутентификации без переписывания утилиты login, а лишь редактируя соответствующий файл конфигурации PAM. Таким образом, можно составить протокол аутентификации, содержащий схемы аутентификации пользователя «по голосу», «по отпечатку пальца», с использованием РИК и т.п. При этом существует возможность задания ряда параметров для каждой схемы, позволяющих определить необходимость успешного прохождения какой-либо схемы. Например, можно добавить схему, в задачи которой входит рекомендация пользователю о необходимости смены пароля. В этом случае смена пароля не является обязательным и, следовательно, схема может завершиться неудачей, однако это ни в коей степени не повлияет на результат всего протокола аутентификации. PAM решает четыре типа задач – управление аутентификацией, управление учетными записями, управление сеансом и управление паролями. Ассоциации между схемами управления и соответствующим приложением задаются в конфигурационном файле. Функции управления реализуются в модулях, указанных в конфигурационном файле.

Данная подсистема включает в себя четыре основных модуля аутентификации и идентификации с использованием специальных средств:

- РИК (российская интеллектуальная карта);

- eToken RIC (аналог РИК в виде USB брелка);
- биометрическая аутентификация пользователя по голосу;
- биометрическая аутентификация по отпечатку пальца.

Подсистема взаимной аутентификации пользователей, вступающих в информационный обмен по сетям связи, реализуется в виде программной библиотеки, используемой приложениями пользователей, вступающих в информационный обмен по сетям связи. При этом ключи аутентификации хранятся в центре сертификации. Для обеспечения однозначной аутентификации участников электронной операции, целостности передаваемых данных и неотрекаемости участников при передаче конфиденциальных данных были использованы отечественные алгоритмы электронной цифровой подписи по ГОСТ Р 34.10-94 и формирования дайджеста сообщения по ГОСТ Р 34.11-94, которые обладают рядом преимуществ по сравнению с зарубежными алгоритмами (исключение составляет алгоритм RSA, так как не существует отечественного стандарта для несимметричных алгоритмов шифрования данных). Схемы аутентификации (идентификации) пользователя с использованием РИК и eToken RIC реализуются в виде системной библиотеки и могут использоваться как вместе с разработанным подключаемым модулем аутентификации (PAM), так и при создании новых программных средств, реализующих механизмы защиты от НСД. Модуль PAM предназначен для аутентификации пользователя в приложениях, использующих сервис PAM, путем предъявления секретного ключа, расположенного на защищенном носителе РИК или eToken RIC.

Кроме того, для работы с РИК и eToken RIC были разработаны библиотеки функций для организации хранения ключей разных типов, которые были использованы в подсистемах криптографической защиты данных и аутентификации пользователей, а также могут служить для создания дополнительных средств защиты информации на основе этих аппаратных средств независимыми разработчиками. Методы аутентификации на основе паролей либо аппаратных ключей достаточно надежны, но имеют довольно серьезные недостатки и прежде всего – возможность использования посторонними лицами, например, вследствие подбора пароля либо хищения аппаратного ключа. Поэтому большой интерес представляют биометрические средства аутентификации пользователей, основанные на их неотъемлемых признаках. В данной работе были представлены две подобные системы – аутентификация по отпечаткам пальцев и аутентификация по голосу.

Особо следует отметить подсистему биометрической аутентификации по голосу, разработанную под руководством доцента каф.БИТ Федорова В.М.

Для создания действительно эффективной системы необходимо было решить следующие задачи: выделение характерных устойчивых признаков, в качестве которых были использованы кепстральные коэффициенты, вычисленные по коэффициентам линейного предсказания; обработка речевого сигнала, состоящая из удаления пауз и шипящих звуков; принятие решения об аутентификации пользователя на основе искусственных нейронных сетей.

В системах аутентификации по голосу пользователь предъявляет системе голос для подтверждения, что этот голос принадлежит данному пользователю, но непосредственное сравнение речевых сигналов невозможно вследствие ряда причин, например, случайного характера некоторых сегментов речи и нерегулярности произношения по амплитуде и времени, поэтому для идентификации субъекта по голосу используют набор устойчивых параметров, выделяемых из речевого сигнала. В качестве таких параметров принято использовать параметр основного тона, кепстральные коэффициенты и значения формант. Наши эксперименты показали, что наибольшей устойчивостью для одного субъекта обладают кепстральные коэффициенты, вычисленные по коэффициентам линейного предсказания.

Предлагаемый метод распознавания использует набор искусственных нейронных сетей (ИНС), число которых равно числу пользователей. Из полученных для каждого пользователя кепстральных коэффициентов набирались обучающие выборки. Каждая ИНС методом ОРО настраивалась на обучающую выборку одного из пользователей системы. При распознавании диктора над тестируемой фразой производится аналогичная предварительная обработка речевого сигнала. Вычисленные кепстральные коэффициенты подавались на входы каждой из нейронных сетей. Одна из сетей благодаря свойству обобщения, полученному на этапе обучения, даст максимальный ответ. Эта сеть считается принадлежащей владельцу данного голоса. По ответам сетей принимается решение об идентификации пользователя. Принятие решения о принадлежности произнесенной фразы к определенному диктору с последующим допуском его в систему или отказе от допуска производится на основе анализа интегральной оценки ответов нейронной сети. Система предусматривает установление порога идентификации диктора.

На основе этой подсистемы можно строить системы безопасности как избирательной, так и полномочной политики доступа. Данная разработка является оригинальной, а полученные результаты превосходят другие подобные системы.

Таким образом, можно выделить два типа механизмов, используемых для аутентификации пользователей в разработанной подсистеме разграничения доступа: вероятностные (биометрические) и детерминированные (основанные на применении аппаратных средств). В подсистеме разграничения доступа существует возможность построения схем, предусматривающих совместное использование различных видов аутентификации. Например, администратор системы защиты от НСД может построить следующую схему аутентификации: пользователь обязательно должен пройти биометрическую аутентификацию по голосу и аутентификацию с использованием РИК или eToken RIC по выбору.

Использование интеллектуальных карт РИК и брелков eToken RIC для хранения ключевой информации

Одним из способов повышения надежности защиты системы от НСД является хранение ключей шифрования и аутентификации на внешних носителях – смарт-картах и брелках. В данной системе брелки и смарт-карты используются в двух назначениях. Первое назначение – использование брелков и смарт-карт в процессе аутентификации. В этом случае в памяти устройства хранится значение хэш-функции от пароля пользователя. При вводе пароля пользователя с клавиатуры по этому паролю вычисляется значение хеш-функции, которое сравнивается с тем, которое хранится на брелке или карте. В случае совпадения этих значений аутентификация считается успешной. В случае их несовпадения аутентификация считается несостоявшейся. Второе назначение смарт-карт и брелков – хранение ключей пользователя, используемых для шифрования различных данных. Для работы с этими ключами разработаны специальные библиотеки работы с устройствами. Всего на одном устройстве может храниться до пяти различных типов ключей – ключи для аутентификации, шифрования файловой системы, шифрования сетевого трафика, шифрования по алгоритму ГОСТ и шифрования по алгоритму RSA. Длина каждого ключа считается равной 256 бит. Всего может храниться до семи ключей каждого типа. Специальная организация структуры памяти смарт-карт и брелков гарантирует надежность хранения ключей. Изначально вся доступная память карточки или брелка занята одним файлом. Этот файл доступен для чтения без ограничений и доступен для записи по паролю. Пароль хранится в другом файле специального вида, доступном по записи без ограничений, но по предъявлению текущего пароля. Все хранимые ключи хранятся внутри основного файла. Ключи хранятся последовательно. Доступ к конкретному ключу может быть полу-

чен по смещению, если известны номер типа ключа и порядковый номер самого ключа. Чтобы исключить возможность чтения незаписанного ключа, в конец памяти добавлена контрольная информация.

Функции библиотеки контролируют местоположение записанных ключей. Невозможно прочитать ключ из памяти устройства, если он был оттуда удален. Также исключается возможность чтения случайной информации из памяти, если туда не был до этого помещен правильный ключ. Такая надежность достигается за счет хранения битовых масок области памяти. Эти битовые маски и другая служебная информация хранятся в специальных областях памяти смарт-карт и брелков и могут быть прочитаны только специальными функциями. Библиотека функций необходима для обеспечения возможности написания приложений, использующих карточки и брелки. Библиотека решает проблемы низкоуровневого взаимодействия с устройствами и предоставляет пользователю-программисту набор функций для работы с ключами, хранимыми на устройствах.

Непосредственная работа с картой возможно только после задания соответствующих параметров обращения к устройству. Работа с карточкой или брелком состоит в последовательном вызове ряда функций управления устройством и передачи данных. В случае использования библиотеки все эти действия скрыты от пользователя, который видит единый интерфейс независимо от того, смарт-карта или брелок используются. Также при использовании специальных функций работы с ключами повышается надежность правильного считывания/записи ключей и обеспечивается контроль за целостностью ключей благодаря специальной организации памяти. Для организации защищенной работы с интеллектуальными картами была разработана подсистема разграничения доступа к информации, хранимой на них, а также средства безопасного обмена данными между картами и приложением, обращающимся к ним за ключевой информацией.

В случае хранения на ИК информации, имеющей высокий уровень конфиденциальности, каждый файл карты может хранить информацию в зашифрованном виде, с указанием протокола шифрования и ключа, на котором зашифрован файл, для каждого конкретного файла. Также ИК может быть сконфигурирована таким образом, что для каждого файла карты будет необходимо указать PIN карты или пароль аутентификации. В таком случае каждому пользователю системы назначаются определенные уровни полномочий, и в соответствии с этими уровнями строится иерархия прав доступа пользователей к файлам ИК. Файлы записываются на ИК в соответствии с указанными правами доступа, шифруются на определенных ключах и доступ к ним возможен после указания пользователем ключа аутентификации. Ключи шифрования и аутентификации могут быть одинаковыми для некоторых групп файлов, например, принадлежащих одному пользователю или имеющих одинаковый уровень секретности (защиты). Для повышения надежности защиты системы от возможного постороннего вмешательства в процесс передачи данных между картой и терминалом может использоваться сертификация передаваемой информации и организация доступа к файлам на основе предъявления сертификатов пользователей. Данные, подлежащие сертификации, шифруются открытым ключом пары ключей шифрования конкретного файла, и поэтому могут быть открыты только на ИК (секретный ключ пары ключей шифрования никогда не покидает карты), и подписываются, используя секретный ключ пары ключей цифровой подписи пользователя. В каждом файле на ИК хранятся: секретный ключ пары ключей шифрования этого файла и открытый ключ пары ключей цифровой подписи пользователя (пользователей), которому разрешен доступ к данному файлу. Раскрытие сертификата происходит следующим образом: сначала ОС карты раскрывает данные сертификата согласно используемому алгоритму шиф-

рования, затем, получая из этих данных имя или идентификатор пользователя, ОС выбирает из базы данных пользователей файла соответствующий открытый ключ пользователя — владельца сертификата. Используя этот ключ, ОС раскрывает цифровую подпись сертификата и удостоверяется, что сертификат на самом деле прислан тем пользователем, который зарегистрирован в базе данных пользователей данного файла и, следовательно, имеет право доступа к содержимому данного файла. Если доступ к данному файлу могут иметь несколько пользователей, то после раскрытия сертификата и установления личности и подлинности личности пользователя — владельца сертификата, операционной системой ИК может быть осуществлено дополнительное разграничение доступа внутри этого файла. Скажем, одним пользователям можно только читать данный файл, а другим, имеющим более высокий уровень допуска, — еще и изменять информацию, хранящуюся в данном файле.

При организации доступа к информации, хранящейся на ИК, при помощи сертификатов пользователей отпадает необходимость идентификации и аутентификации пользователя при попытке доступа к файлу. Это становится возможным, поскольку правильность сертификата (то есть, по сути, знание пользователем своего секретного ключа и открытого ключа файла, к которому он собирается произвести доступ) и говорит о том, что этот пользователь является корректно зарегистрированным для системы и для данного файла. С учетом созданных дополнительных подсистем защиты была доработана стандартная подсистема аудита, для чего был разработан специальный демон регистрации и учета событий.

Выводы

Таким образом, реализация предложенных подсистем криптографической защиты данных и взаимной аутентификации пользователей позволила создать систему обработки данных на базе LINUX-подобных систем с высоким уровнем защищенности (в частности, если в качестве базовой используется ОС МСВС 3.0, то уровень защищенности соответствует классу 1А по требованиям Гостехкомиссии к защите информации в автоматизированных системах).

Работа поддержана грантом РФФИ №03-07-90075.

Л.К. Бабенко, О.Б. Макаревич, О.Ю. Пескова
Россия, г. Таганрог, ТРТУ

РАЗРАБОТКА КОМПЛЕКСНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК

Обнаружение атак – это искусство выявления несоответствующего, неправильного или аномального поведения пользователя или процесса. Обнаружение атак стало насущной проблемой, потому что в современных вычислительных системах невозможно сохранить защищенность с помощью традиционных методов защиты, применяемых ранее, когда компьютеры были уязвимы только со стороны «внутреннего врага». Постоянно расширяется число уязвимостей и атак в существующем системном и прикладном программном обеспечении, растет число людей, из озорства или из коммерческих целей атакующих информационные системы. Перед коллективом разработчиков была поставлена задача разработать комплекс средств обнаружения атак, позволяющий обнаруживать и распознавать атаки различного происхождения и различной направленности. Одним из бастионов защиты, предохраняющих информационные системы как раз от внешнего врага, являются системы обнаружения атак (СОА - Intrusion Detection System, IDS), функционирующие на сетевом уровне. Целью таких систем являются обнаружение и идентификация нарушителей, а также их блокировка до того момента, когда атака успела нанести вред системе и может быть обнаружена с помощью средств монито-