Аппаратно-программные комплексы защиты

Умные защитники

Ограничение несанкционированного доступа к компьютеру — сложная и комплексная задача, поэтому обеспечить должный уровень защиты только механическими способами зачастую довольно непросто. В этом случае на помощь придут аппаратно-программные комплексы, которые в последнее время получают все большее распространение.

Если говорить об устройствах и технологиях, позволяющих наладить и обезопасить процесс идентификации или авторизации пользователей, то нельзя не упомянуть о смарт-картах и других подобных им защитных средствах. За возможностями большинства из них лежит технология PKI (Public Key Infrastructure), или инфраструктура открытого ключа — система, в которой пользователи и транзакции аутентифицируются по методу шифрования с открытым ключом. При этом используется пара ключей: открытый (public) и частный (private), а также цифровой сертификат, содержащий имя пользователя, и сертификат полномочия (certificate authority) для управления всеми вышеуказанными составляющими. В то время как частный ключ хранится все время на носителе, открытый ключ пользователя может быть распознан стороной, производящей идентификацию.

В общем случае определение полномочий пользователя и его идентификация проходят по следующему сценарию: информация о пользователе считывается специальным приспособлением — ридером (reader), вводится »

код для активации устройства, после чего ридер может использовать частный ключ для подписи документов, аутентификации пользователя и проведения прочих транзакций, требующих мер защиты.

Открытый ключ может быть использован контролирующей стороной для проверки цифровой подписи пользователя, шифрования информации, предназначенной для прочтения только конкретным пользователем, или для применения аутентификационного протокола «ответной реакции», подтверждающего то, что смарт-устройство пользователя действительно «знает» соответствующий частный ключ. Очевидно, что устройства, реализующие данные технологии, подходят для использования в тех случаях, когда предъявляются серьезные требования к мерам обеспечения защиты.

В прошлом технология PKI была воспринята довольно холодно из-за своей сложности, а также особых требований к разработке смарт-продуктов. Принятие таких стандартов как XKMS (XML Key Management Specification) и SAML (Security Assertion Markup Language) в определенной степени помогло решить проблемы совместимости и упростить жизнь разработчикам. Теперь они могут использовать для своих целей продукты действующих эмитентов карт, в числе которых Visa, Master Card, American Express, либо выпустить собственные карты, используя поставщиков вроде Schlumberger или Gemplus.

Карты, деньги, два стола

Наверное, самыми популярными среди вышеописанных устройств являются смарт-карты. По своим размерам и внешнему виду они напоминают обычные кредитные карточки. Смарт-карта содержит интегрированный микрочип, а для передачи информации с карты или на карту требуется специальное устройство — ридер, который электронным образом соединяет микропроцессор карты с устройством, передающим в карту или принимающим из нее информацию. Впрочем, доступ к смарт-картам может осуществляться и бесконтактным способом при помощи радиосигналов.

Принято выделять два основных типа карт: карты памяти и процессорные карты (также известны как криптографические). Первый тип признан менее надежным средством обеспечения безопасности, поскольку основная его функция заключается в том, чтобы просто хранить цифровую информацию. Процессорная карта, как следует из названия, содержит в себе микропроцессор, который может использоваться для решения более сложных задач. Она может быть сконфигурирована так, что частный ключ не будет показан никому, поскольку он защищается криптографическими методами на уровне самой карты. Процессорные карты способны проводить сложную обработку информации для реализации защиты доступа. Обычная карта вынуждена списывать с себя частный ключ каждый раз, когда требуется провести криптографическую операцию, что чревато перехватом ключа.

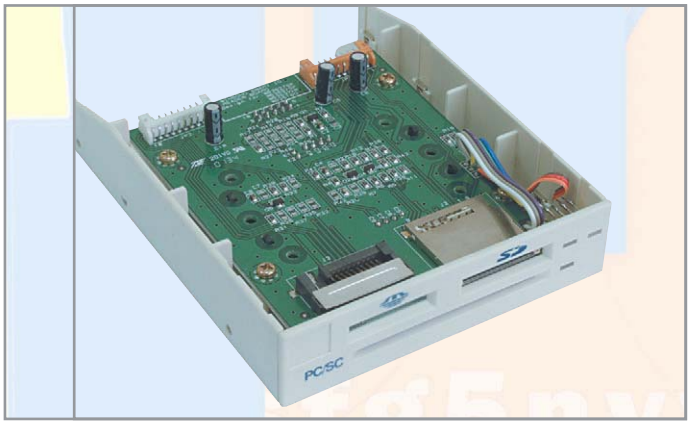
Криптография является средством защиты пароля, но иногда объектом нападения становится именно карта. Для этого и существуют способы защиты самой смарт-карты: например, иногда их оснащают различными датчиками, фиксирующими как физическое воздействие, так и диагностирующими само состояние карточки (например, изменение напряжения питания или тактовой частоты процессора). Существуют также и другие ме-

Российская разработка

«Пушной» защитник

Разработка отечественного производителя (НИП «Иноформзащита») под названием «Соболь» поможет сохранить годовой баланс предприятия в целости и сохранности. Устройство классифицируется как электронный замок с возможностями идентификации и аутентификации пользователей, регистрации попыток доступа к компьютеру, запрета загрузки ОС со съемных носителей и осуществления контроля за целостностью программной среды. Плата, являющаяся одним из компонентов комплекса, устанавливается в ISA- или PCI-слот. В последнем случае при попытке несанкционированного доступа аппаратно блокируется до трех устройств. Определение пользователей и протоколирование попыток доступа не зависят от типа используемой ОС. Стоит также отметить, что в электронном замке используются идентификаторы Touch Memory фирмы Dallas Semiconductor. Задача защитного комплекса состоит в проверке идентификационных данных пользователя, которые выдаются администратором и затем регистрируются в системе «Соболь». Служебная информация о пользователе (имя, номер присвоенного персонального идентификатора и т. д.) хранится в энергонезависимой памяти электронного замка. Стоит отметить большие возможности устройства для администрирования и возможность комбинирования с прочими охранными комплексами, например с аппаратно-программным комплексом «Континент-К» и системой защиты информации Secret Net, производимыми тем же предприятием.

▲ Ридеры для смарт-карт бывают как внешние, так и внутренние, и зачастую выглядят очень приятно и привлекательно



▲ С материнскими платами все чаще начинают поставляться ридеры для смарт-карт и носителей на флеш-памяти

USB-токенами для ограничения доступа к компьютеру и мобильными телефонами, способными работать со смарт-картами, сегодня уже мало кого можно удивить

тоды защиты карт вроде логического и физического контроля четности во всем поле энергонезависимой памяти карты. Как следствие, для обеспечения санкционированного доступа к компьютерной технике, а также в иных целях безопасности чаще всего используется микропроцессорный тип смарт-карт.

Преимущества смарт-карт заключаются в том, что они обладают самыми распространенными конструктивными характеристиками для систем охраны. Несомненным плюсом является также и то, что на рынке представлено много продуктов, доказавших состоятельность примененного подхода.

«Золотые ключики» — USB-токены

Следующими в классе «умных» устройств идут токены. Как и смарт-карты, данные устройства могут быть процессорными картами либо играть роль карт памяти, реализующих все преимущества PKI-технологии. По своим конструктивным характеристикам они напоминают брелоки для ключей и могут подключаться к настольным и переносным компьютерам через USB-порт. Эти маленькие «ключики» позиционируются как эффективная мера защиты приложений и сетевых сервисов, например частных виртуальных сетей, а также для контроля над доступом в Интернет, интранет и т. п.

Вообще, подобных устройств выпускается великое множество, в частности, известная фирма Aladdin Software Security R.D., которая в основном занимается разработкой средств защиты ПО, делает подобные токены, которые используются при авторизации как в различных приложениях, так и при доступе к самому компьютеру.

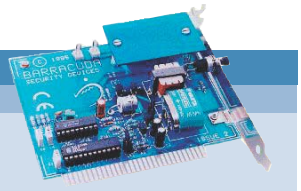
Разберем подробнее принцип работы и состав таких приспособлений на примере изделий от компании Rainbow. «Брелок» содержит в себе два важных компонента: USB- и криптографический контроллеры. Криптографический чип состоит из микроконтроллера, математического ускорителя для шифровальных операций с открытым ключом, аппаратного ускорителя для некоторых видов шифрования, участка ROM-памяти для операционной системы устройства, памяти для регистров ввода-вывода, программируемой памяти и генератора псевдослучайных чисел. Если сравнить данные устройства со смарт-картами, то роль ридера в данном случае выполняет встроенный USB-контроллер.

К достоинствам данных приспособлений относятся их более низкая стоимость по сравнению со смарт-картами, отсутствие необходимости использовать ридер, простоту установки. К недостаткам — необходимость наличия свободного USB-слота и проблемы совместимости с остальными технологиями идентификации.

В комплекте с материнской платой

Вопросами обеспечения безопасности занимаются не только производители сугубо охранных устройств, но и некоторые фирмы — производители компьютерных комплектующих. Прекрасным примером здесь может служить MicroStar International (MSI), чьи материнские платы комплектуются опциональным устройством под названием Smart Key, представляющим собой как раз устройство из класса USB-токенов.

Радикальная охранная система

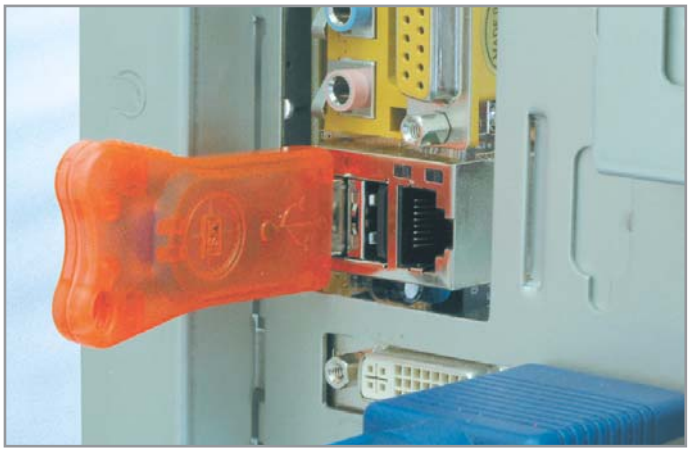


Хищная рыбка

В свое время специалистами одной из английских компаний было разработано достаточно интересное устройство под названием Barracuda Security Device. Оно представляет собой плату размером 105x100 мм, устанавливающуюся в ISA- или PCI-слот. Одно такое устройство может использоваться как для защиты только одного компьютера, так и для охраны локальных сетей. Достигается это за счет специально разработанного программного обеспечения, входящего в состав охранного пакета. С его помощью сигнализация, установленная на центральной рабочей станции, способна следить за сотнями компьютеров. В момент совершения преступления охранный комплекс может связаться с администратором не только через сеть, но и передать ему сигнал на пейджер и даже на мобильный телефон.

Подробнее остановимся на составных частях комплекса. Во-первых, это автономный источник питания, так что даже если компьютер отключен, он остается под защитой. Во-вторых, внутренний датчик движения, активирующий при нелегальном передвижении сирену громкостью 120 дБ. В-третьих, внутренний световой датчик, отслеживающий уровень освещенности внутри компьютера и при малейшем ее изменении запускающий сигнализацию. Помимо всего прочего, если крышка корпуса была снята без ввода специального PIN-кода, активируется еще и капсула со специальной несмываемой краской, покрывающей внутрикомпьютерное пространство. Для страховки есть еще один датчик, аналогичный тем, которые применяются для защиты окон, только в этом случае он ставится на корпус. В итоге у злоумышленника не остается никаких шансов!

▲ Это нехитрое с виду приспособление способно надежно оградить ваш компьютер от попыток несанкционированного доступа



▲ Smart Key, установленный в USB-порте материнской платы. Как только он будет вынут, загрузить компьютер не удастся

Производитель позиционирует данное приспособление как средство защиты с высокой степенью надежности: никто не сможет воспользоваться компьютером, кроме владельца ключа. Кроме того, часто Smart Key предоставляется как бесплатное приложение к материнской плате, и, по заявлениям самой MSI, таким образом пользователь экономит $60. Комплект поставки этого защитного устройства состоит из шнура-удлинителя для USB (нужен для облегчения доступа к USB-порту на задней панели корпуса) и самого ключа. Необходимое программное обеспечение находится на диске, поставляемом вместе с материнской платой.

Установка происходит следующим образом: при отключенном питании компьютера ключ вставляется в порт USB, после чего следует включить компьютер и начать процедуру настройки BIOS, которая автоматически распознает наличие ключа и сама предложит активировать его. При утвердительном ответе появится сообщение с просьбой ввести пароль (не более восьми символов). После подтверждения пароля система сгенерирует набор случайных идентификаторов, которые будут записаны в BIOS и микрочип ключа. Завершив эту операцию, система перезапустится, и произойдет загрузка операционной системы. Далее можно приступать к установке программного обеспечения, работающего под всеми основными версиями ОС Windows.

ПО представлено небольшой утилитой, после установки отображающейся иконкой в системном трее. Утилита запускается только в том случае, если функция Smart Key была активирована в BIOS. В этом программном приложении есть две основные опции, позволяющие настроить все предоставляемые функции должным образом. «Security Settings» позволяет автоматически проводить процедуру авторизации во время входа в Windows — при активации этой функции пользователю не будет нужно постоянно вводить свой логин и пароль. «Other» — содержит еще два пункта: «Disable Screen Saver», «Set Screen When System Locked». В первом пункте есть выбор: включать или нет экранную заставку, когда система блокируется, то есть Smart Key вынут. Соответственно, во втором пункте устанавливается тип выводимой картинки. С этого момента можно считать, что система защиты функционирует на полную мощность.

Подведем промежуточный итог. Защита системы осуществляется двумя способами: применением пароля и ключом в порту USB. Однако здесь есть два важных нюанса. Забыть пароль активации ключа не так уж сложно, особенно учитывая то, что зачастую вводить его приходится только при начальной установке. В этом случае вам, скорее всего, придется обратиться к авторизованному дистрибьютору для того, чтобы вернуть материнскую плату в рабочее состояние. Помимо того, пароль может быть необходим при использовании другого ключа Smart Key или активации нового ключа взамен утерянного или украденного старого. Новый ключ, кстати, можно приобрести через официального дистрибьютора MSI. Наверное, вы уже заметили, что мы упомянули об авторизации при помощи другого, не входящего в комплект данной материнской платы, ключа Smart Key. Отсюда вытекает, пожалуй, основной недостаток данного охранного приспособления. Действительно, в случае использования нового или чужого ключа необходимо знание только пароля, указанного при активации оригинального ключа. Система сама запросит этот пароль при первой загрузке с новым ключом. Если пароль указан правильно, данные из системного BIOS будут перезаписаны в новый ключ, после чего система будет функционировать по-прежнему. Если же пароль трижды указан неверно, система блокируется, и после этого, скорее всего, понадобится визит к дистрибьютору или дилеру MSI. Из всего вышесказанного можно сделать вывод о том, что защита системы значительной своей частью обеспечивается паролем, который, в свою очередь, также нуждается в защите.

Наследство Маркони

Теперь поговорим о бесконтактных смарт-устройствах, производящих идентификацию при помощи радиочастоты. К комплексам такого типа можно отнести, например, Link-IT — продукт совместных усилий компании Secure-It Inc и Wavetrend. Link-IT использует технологию RFID (Radio Frequency Identification) — идентификацию посредством радиочастот. Система состоит из Tag Reader (приемника метки), Identification Tag (идентификационной метки) и особого программного средства для обеспечения надежности доступа.

Создатели данной охранной системы утверждают, что их детище обладает следующими ключевыми особенностями: реализована защита от доступа к данным несанкционированного пользователя; компьютер становится неработоспособным в случае, если ключ потерян или украден, без ассоциированной именно с ним метки; в специальном файле осуществляется протоколирование всех действий пользователей; обеспечена полная совместимость с Microsoft Windows 9x, 2000, NT, XP.

▲ USB-ридер, входящий в комплект системы «Мастер паролей», весьма компактный и неплохо смотрится будучи прикреплен-ным к монитору

▲ Программная часть «Мастера паролей» обладает удачным и продуманным интерфейсом, так что разобраться в ней не составляет труда

» Работа с комплексом начинается с установки приемника метки в последовательный порт компьютера (хотя разрабатывается версия и под USB-порт) и инсталляции прилагаемого программного обеспечения. Приемник меток сразу же произведет сканирование окружающего пространства на предмет обнаружения всех совместимых меток, а результаты будут занесены в файл протокола. Теперь компьютер сможет функционировать только в том случае, если сигнал идентификационной метки находится в радиусе его обнаружения. Как только сигнал теряется, например оператор отлучается на обед, программная часть комплекса запускает свою защитную экранную заставку. Время, через которое это происходит, настраивает сам пользователь, оно может быть в пределах от 10 с до 5 мин. При таком положении дел даже нажатие сочетания клавиш «Ctrl+Alt+Del» и полное отключение питания не поможет потенциальному злоумышленнику получить доступ к информации, хранящейся на компьютере. Таким образом, доступ к нему полностью заблокирован до тех пор, пока не вернется пользователь с меткой, разрешающей доступ. Кстати, программная часть Link-IT способна также организовывать режим работы одного компьютера с несколькими метками.

Преимуществом технологии являются возможность организации доступа не только согласно иерархии «администратор-пользователь», но и при помощи системы паролей. К интересным особенностям рассматриваемого продукта можно также отнести возможность работы компьютера только в строго определенном местоположении. Функционирование в таком режиме становится возможным при применении дополнительной метки, фиксирующей положение ПК. Механизм идентификации в этом случае немного изменится. Для того чтобы производительность охранной системы была оптимальной, приемник меток должен зафиксировать присутствие минимум двух авторизованных меток — зарегистрированного пользователя и метки положения. Последняя устанавлива- »

Смарт-карта на защите софта

Копилка для паролей

Смарт-карты успешно применяются и для авторизации и ограничения доступа к различным программам. Примером тому служит отечественная разработка компании RusCard под названием «Мастер паролей». Этот комплекс является инструментом для хранения и ввода паролей в среде Windows. Сфера его применения — обеспечение информационной безопасности. Основными составляющими являются смарт-карта, ридер и программное обеспечение. Функционирует решение следующим образом: запускается любое Windows-приложение, требующее идентификационные данные. Далее при помощи «Мастера паролей» на карточке создается учетная запись. В этом случае можно воспользоваться готовым шаблоном, находящимся в коллекции «Менеджера паролей» — программного компонента комплекса, — либо использовать универсальный тип записи, в котором указываются вводимые идентификаторы, а также месторасположение этой информации в окне программы. Пароль, по заверениям разработчиков, может быть длиной до двух тысяч символов и использовать латиницу, русский алфавит и набор специальных символов. Теперь, когда приложение в следующий раз запросит пароль, нужно будет вставить карту в ридер, и необходимые поля заполнятся сами. Пароли, в свою очередь, хранятся только на смарт-карте и ни в каком виде не остаются на компьютере. К преимуществам этой системы можно отнести также и то, что на карте может храниться не одна учетная запись, содержащая пароли, и что все их можно защитить PIN-кодом, так же как и саму карту. Производители системы постарались позаботиться о конечном пользователе. Доказательством того является факт существования нескольких исполнений ридеров: внешние подключаются через USB, COM (для передачи данных) + PS/2 (для подачи питания), а внутренние — через платы для ISA- или PCI-слотов.

Подведем итог: «Мастер паролей» может быть действительно применен для обеспечения защиты, хотя точнее было бы сказать — для обеспечения сохранности идентификационной информации и для «приватности» ввода этой самой информации. Но как средство ограничения доступа к компьютеру ее рассматривать все же, пожалуй, нельзя.

▲ Без идентификационной метки поработать с этим ноутбуком вам не удастся

» ется в рабочем помещении за навесными потолками или под крышкой офисного стола. Соответственно, при удалении или перемещении компьютера из заданного помещения доступ к нему блокируется, даже если метка оператора присутствует в зоне обнаружения.

Далее мы рассмотрим отдельные элементы этого интересного комплекса с описанием их функциональных возможностей.

Особенности функционирования Link-IT

Tag Reader (приемник метки) работает на обнаружение меток для выявления присутствия определенных людей или объектов. Приемник получает идентификационный пакет данных, передаваемый идентификационной меткой, и декодирует зашифрованный сигнал по следующему алгоритму: радиочастота преобразуется в цифровые данные, которые поступают в программную часть системы. Радиус обнаружения меток варьируется в пределах 1,5–4,5 м. Если в процессе работы приемник отключится от порта, то произойдет то же самое, что и в случае удаления сигнала метки за радиус обнаружения — система автоматически войдет в режим охраны.

Identification Tag (идентификационная метка) — средство организации упорядоченной системы доступа, однозначно отделяющей, например, простых пользователей от системного администратора. Это устройство чаще всего выполняется в виде пластиковых карт, по сути представляя собой небольшой передатчик. Питание его происходит за счет внутренней батареи, рассчитанной на 5 лет использования. Из-за того, что данный комплекс хорошо подходит для защиты сверхсекретных приложений, передача сообщений между самой меткой и приемником шифруется, дабы избежать клонирования, копирования и эмуляции метки. А так как часто требуется, чтобы приемник мог опознавать сразу несколько идентификационных меток в поле своего обнаружения (всего с одним компьютером могут работать 32 дополнительных пользователя, помимо одной администраторской метки и одной метки основного пользователя), используется специальный алгоритм. Метка Link-IT передает 35-байтное идентификационное сообщение, состоящее из центрального кода и последовательного идентификационного номера. В принципе, и тот и другой могут задаваться покупателем системы, однако для программирования меток придется обратиться в фирмы-производители. В дополнение к определению идентификационной информации можно приобрести особые варианты исполнения передатчиков меток с различными датчиками (на удар, движение), повышающими надежность системы. Существует два основных типа меток: Slimline и Industrial. Передатчики меток версии Slimline считаются более помехоустойчивыми, так как могут работать без сбоев даже будучи прикрепленными к металлическим поверхностям. Индустриальная метка может передавать свой сигнал на меньший радиус, но с использованием опциональной внешней антенны расстояние передачи радиосигнала может быть увеличено до 8 метров.

Заключение

Каждому из нас самому решать, какие устройства использовать для защиты компьютера и использовать ли их вообще. У нас в стране, похоже, если и не пренебрегают средствами защиты компьютерной и офисной техники, то уж точно широко не рекламируют их. Мы же хотели бы посоветовать тем, кто захотел обзавестись подобными устройствами, не останавливаться на установке только какого-то одного типа устройств. Например, механические средства защиты можно сравнить с изюмом, который хорош не столько сам по себе, сколько как добавка, например, в булочки, то есть как поддержка программно-аппаратных средств охраны.

Из всех рассмотренных методов защиты особо хотелось бы отметить решения MSI, чьи материнские платы уже сейчас практически серийно оснащаются средствами защиты с достаточно высокой степенью надежности.

■ ■ ■ Андрей Шепелев