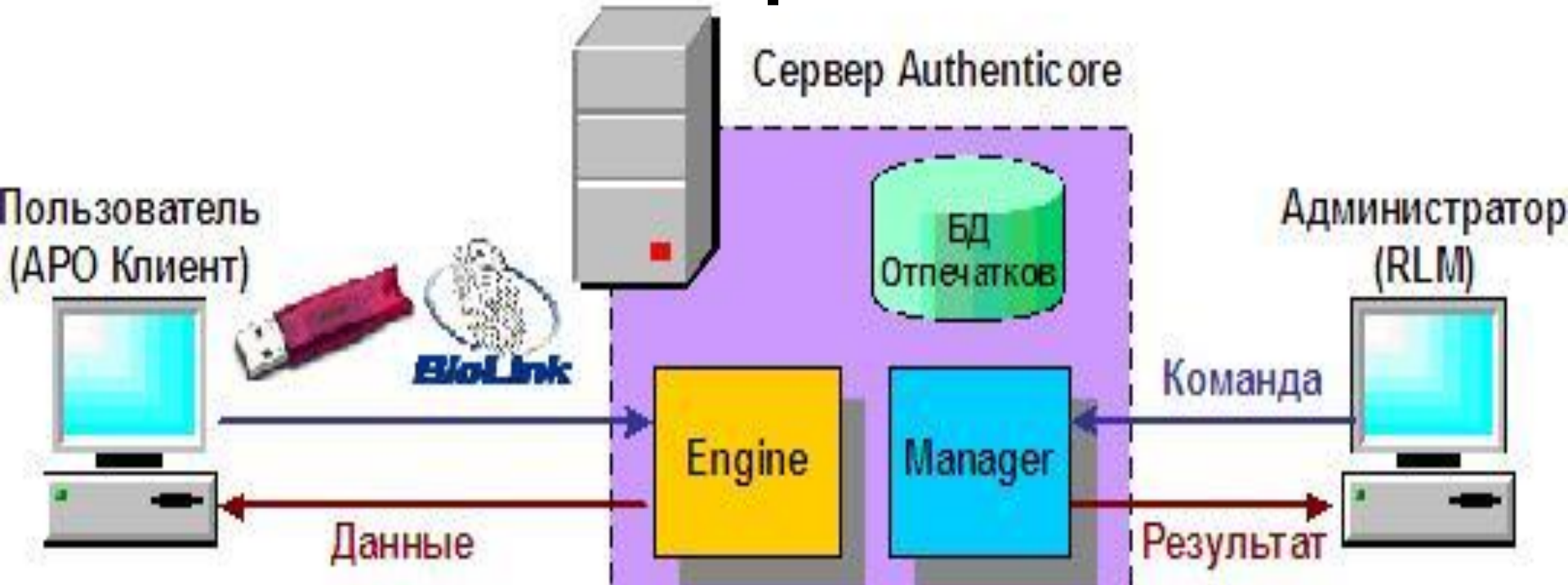
Аппаратные ключи защиты



- *Первоначально аппаратные ключи были созданы как средство борьбы с несанкционированным копированием программных продуктов, но в дальнейшем сфера их применения значительно расширилась...*

- Большинство компьютерных программ распространяется по принципу владения оговоренным количеством рабочих копий (в простейшем случае — только одной). Естественно, общепринятый в международной практике термин «защита от копирования» достаточно условен, так как практически всегда можно переписать информацию, находящуюся на носителе, и сделать сколько угодно ее резервных копий. Другое дело, что для сохранения коммерческих и авторских прав разработчиков программа все равно должна выполняться только на одном компьютере.

- Таким образом, фактически защита от копирования для программного обеспечения — это невозможность выполнения программы на большем числе компьютеров, чем разрешено ее разработчиками и распространителями по данному договору. Следовательно, для сохранения прав необходимо наличие средств, дающих возможность защиты от несанкционированного выполнения — чтобы без санкции разработчика или фирмы-распространителя невозможно было получить работоспособный программный продукт.

- Наиболее распространенным и надежным способом защиты от несанкционированного запуска стали программно-аппаратные ключи, подключаемые к COM-, LPT- или USB-портам. Почти все коробочные варианты серьезного коммерческого ПО используют программно-аппаратные комплексы защиты, более известные как аппаратные ключи защиты.

- Такие способы защиты основаны на том, что в компьютер добавляется специальное физическое защитное устройство, к которому при запуске защищаемой программы обращается ее контролирующая часть, проверяя наличие ключа доступа и его параметров. Если ключ не найден (устройства обычно формируют еще и код ответа, который затем анализируется программой), то программа не запустится (или не будет разрешен доступ к данным).

- Общий принцип работы компьютера в этом случае следующий. После запроса на выполнение защищаемой программы происходят ее загрузка в оперативную память и инициализация контролирующей части. На физическое устройство защиты, подсоединенное к компьютеру, посылается запрос. В ответ формируется код, посылаемый через микропроцессор в оперативную память для распознавания контролирующей частью программы. В зависимости от правильности кода ответа программа либо прерывается, либо выполняется.
- кредитная смарт-карта или электронные деньги.

- В дальнейшем сфера применения таких ключей значительно расширилась. Сегодня этот ключ используется для идентификации владельца, для хранения его личной электронной подписи, конфиденциальной информации, а также как

- Таким образом, мы имеем сегодня недорогое средство для широкомасштабного внедрения смарт-ключей в качестве персональных идентификаторов или в составе так называемых AAA-систем (аутентификация, авторизация и администрирование). До сих пор предлагалось оснащать компьютеры специальными считывателями, что, конечно, нереально.

- Современные устройства биометрической аутентификации пользователей (столь часто показываемые в голливудских фильмах) типа систем, работающих с отпечатками пальцев или со снимками радужной оболочки глаза, стоят настолько дорого, что не найдут широкого практического применения. При этом в любом случае следует помнить, что абсолютно надежной защиты не существует. Любую защиту можно сломать, поэтому необходимо искать оптимальное соотношение затрат на создание защиты и прогнозируемых затрат на ее взлом, учитывая также ценовое соотношение с самими защищаемыми продуктами.

- Наилучшим решением, по мнению экспертов, являются смарт-карты — их невозможно подделать, вероятность сбоя в работе практически исключена, аутентификация пользователя производится на локальной рабочей станции, а не на сервере, то есть исключена возможность перехвата информации в сети и т.д.

- Единственным недостатком смарт-карты может быть только необходимость специального карт-ридера (устройства считывания), но эту проблему решают устройства, интегрированные со считывателем, которые подключаются напрямую к USB-порту. Эти небольшие высокотехнологичные устройства обеспечивают авторизацию владельца в компьютерных системах, осуществляют безопасное хранение сертификатов, электронных подписей и т.д. и могут использоваться в электронных платежных системах (электронных «кошельках» для Интернета).

- Сегодня все острее встает проблема обеспечения безопасности при использовании сетевых технологий и все более насущной становится потребность в решениях по защите мобильных пользователей. Появляются и беспроводные аппаратные ключи защиты приложений, работающие по технологии Bluetooth. Так, тайваньская компания First International Computer продемонстрировала PDA с соответствующим модулем и беспроводной аппаратный ключ защиты приложений BlueGenie, разработанный в сотрудничестве с Silicon Wave.

HASP

- Одним из наиболее распространенных в России защитных устройств такого типа является устройство HASP (Hardware Against Software Piracy) от компании Aladdin, по сути ставшее стандартом де-факто. Aladdin Software Security R.D. — это российская компания, представитель мирового лидера в области разработки и производства систем аутентификации, защиты информации при работе с Интернетом и защиты программного обеспечения от несанкционированного использования Aladdin Knowledge Systems Ltd.

- HASP — это аппаратно-программная инструментальная система, предназначенная для защиты программ и данных от нелегального использования, пиратского тиражирования и несанкционированного доступа к данным, а также для аутентификации пользователей при доступе к защищенным ресурсам. В первых версиях это небольшое устройство подключалось к параллельному порту компьютера. Затем появились USB-HASP-устройства.

- Иметь маленький USB-ключ значительно удобнее, чем большой 25-штырьковый сквозной разъем, да и часто возникающие проблемы с совместимостью ключей и устройств, работающих через параллельный порт, типа принтеров и ZIP-дисководов изрядно утомляли пользователей. А с USB-устройствами работает автоматическое подключение (plug-and-play), порты USB выносятся на переднюю панель, встраиваются в клавиатуру и монитор. А если даже такого удобного разъема под рукой нет, то в комплекте с этими ключами часто продают удлинители. Существуют несколько разновидностей ключей — с памятью, с часами и т.д.

Основой ключей HASP является специализированная заказная микросхема

Основой ключей HASP является специализированная заказная микросхема

- — ASIC (Application Specific Integrated Circuit), имеющая уникальный для каждого ключа алгоритм работы. Принцип защиты состоит в том, что в процессе выполнения защищенная программа опрашивает подключенный к компьютеру ключ HASP. Если HASP возвращает правильный ответ и работает по требуемому алгоритму, то программа выполняется нормально. В противном случае, по усмотрению разработчика программы, она может завершаться, переключаться в демонстрационный режим или блокировать доступ к каким-либо функциям программы.

Используя память ключа, разработчик может:

- управлять доступом к различным программным модулям и пакетам программ;
- назначать каждому пользователю защищенных программ уникальный номер;
- сдавать программы в аренду и распространять их демо-версии с ограничением количества запусков;
- хранить в ключе пароли, фрагменты кода программы, значения переменных и другую важную информацию.

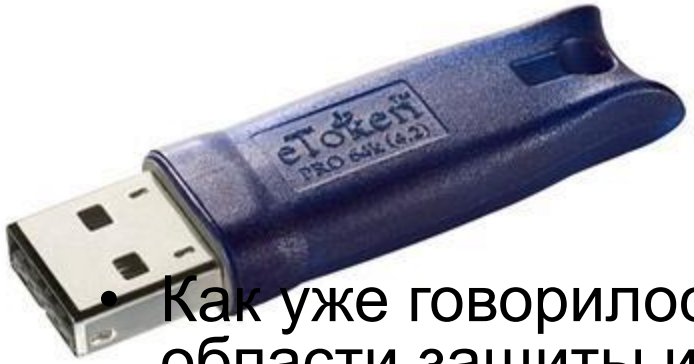
- У каждого ключа HASP с памятью имеется уникальный опознавательный номер, или идентификатор (ID-number), доступный для считывания защищенными программами и позволяющий различать пользователей. Идентификатор присваивается электронному ключу в процессе изготовления, что делает невозможным его замену, но гарантирует надежную защиту от повтора. С использованием идентификатора можно шифровать содержимое памяти и использовать возможность ее дистанционного перепрограммирования.

Hardlock

- Hardlock — это электронный ключ компании Aladdin, предназначенный для защиты приложений и связанных с ними файлов данных, позволяющий программировать ключи защиты и лицензировать авторское программное обеспечение. Механизм работы ключей Hardlock базируется на заказном ASIC-чипе со встроенной EEPROM-памятью.
- Чип имеет сложную внутреннюю организацию и нетривиальные алгоритмы работы. Логику работы чипа практически невозможно реализовать с помощью стандартных наборов микросхем, его очень сложно воспроизвести, а содержащийся в его памяти микрокод — считать, расшифровать или эмулировать.

- Такие ключи могут устойчиво работает во всех компьютерах (включая ноутбуки), на различных портах, в самых разных режимах, позволяя подключать через них практически любые устройства — принтеры, сканеры, модемы и т.п. А малый ток потребления позволяет каскадировать любое количество ключей.
- Hardlock осуществляет защиту 16- и 32-разрядных приложений и связанных с ними файлов данных в прозрачном режиме. При чтении данные автоматически расшифровываются, при записи — зашифровываются с использованием заданного аппаратно-реализованного алгоритма. Эта возможность может использоваться также для хранения и безопасной передачи информации в сети Интернет.

eToken



- Как уже говорилось, наилучшим решением сегодня в области защиты информации являются смарт-карты, но для их использования необходимы специальные устройства считывания (карт-ридеры). Эту проблему снимают устройства типа eToken — электронные смарт-ключи производства той же компании Aladdin, подключаемые напрямую к USB-порту.
- eToken — это полнофункциональный аналог смарт-карты, выполненный в виде брелока. Он напрямую подключается к компьютеру через USB-порт и не требует наличия дорогостоящих карт-ридеров и других дополнительных устройств. Основное назначение eToken — аутентификация пользователя при доступе к защищенным ресурсам сети и безопасное хранение цифровых сертификатов, ключей шифрования, а также любой другой секретной информации.

- Каждому брелоку eToken можно присвоить уникальное имя, например имя его владельца. Чтобы узнать имя владельца eToken, достаточно подключить брелок к USB-порту и открыть окно «Свойства». Однако получить доступ к защищенной памяти eToken и воспользоваться этим брелоком без знания специального PIN-кода нельзя.
- Кроме того, eToken выполнен в прочном водонепроницаемом корпусе и защищен от воздействия окружающей среды. Он имеет защищенную энергонезависимую память (модели PRO и RIC снабжены микропроцессором). Небольшой размер позволяет носить его на связке с ключами.

- Если нужно подключить к компьютеру несколько ключей одновременно, а USB-портов не хватает, то можно воспользоваться концентратором (USB-HUB). Для удобства применения eToken поставляется вместе с удлинителем для USB-порта.
- Таким образом, eToken может стать универсальным ключом, легко интегрируемым в различные системы для обеспечения надежной аутентификации. С его помощью можно осуществлять безопасный доступ к защищенным Web-страницам, к сетям, отдельным приложениям и т.д. Универсальность применения, легкость в использовании, удобство для пользователей и администраторов, гарантированное качество делают его прекрасным средством при необходимости использовать цифровые сертификаты и защищенный доступ.

Secret Disk

- В случае если объем конфиденциальной информации довольно значителен, можно воспользоваться устройством Secret Disk, выполненным с применением технологии eToken. Secret Disk — это разработка компании Aladdin Software Security R.D., предназначенная для защиты конфиденциальной информации на персональном компьютере с ОС Windows 2000/XP.

- Принцип защиты данных при помощи системы Secret Disk заключается в создании на компьютере пользователя защищенного ресурса — секретных дисков, предназначенных для безопасного хранения конфиденциальной информации. Доступ к этой информации осуществляется посредством электронного ключа eToken, подсоединяемого к USB-порту компьютера.

- Доступ к информации, защищенной системой Secret Disk, получают только непосредственный владелец информации и авторизованные им доверенные лица, имеющие электронный ключ eToken и знающие его PIN-код. Для других пользователей защищенный ресурс будет невидим и недоступен. Более того, они даже не догадаются о его наличии.

- Устанавливая на компьютере систему Secret Disk, пользователь может быть уверен в сохранности защищаемых данных. Конфиденциальная информация не может быть просмотрена, скопирована, уничтожена или повреждена другими пользователями. Она не может быть использована посторонними при ремонте или краже компьютера, а также при утере съемного зашифрованного диска.

- Для защиты корпоративных серверов используется специальная версия — Secret Disk Server. Особенностью системы Secret Disk Server также является отсутствие следов закрытого «контейнера с информацией» в файловой системе. Таким образом, если злоумышленники снимут диск с вашего сервера, то они не только не смогут расшифровать данные — они даже не увидят, где именно находится информация.

Заключение

- Аппаратно-программные средства защиты выпускаются в достаточном количестве (помимо лидера — компании Aladdin и другими производителями, в том числе и российскими). Однако если говорить о программном обеспечении, то, пожалуй, единственным способом надежной защиты является перевод ее разработки из разряда ПО в разряд платформ. Иными словами, достаточно сложный программный комплекс требует при эксплуатации тесного сотрудничества с производителем.

- Купить продукт легко, гораздо труднее правильно настроить его и поддерживать. Естественно, такой подход легко реализуем для систем корпоративного назначения, но плохо применим к коробочным программам для широкого пользователя. Однако и в этом направлении работы уже давно ведутся (подписка на ПО, мультимедийные программы с онлайновым обращением и пр.), и производитель получает дополнительные возможности для улучшения защиты.

- Что касается проблем аутентификации, то все чаще применяется технология PKI (Public Key Infrastructure), использующая системы сертификатов и специальных серверов для их проверки — центров сертификации CA (Certification Authorities). Одни из самых популярных систем сертификации — RSA Keon, Baltimore, Verisign и Entrust, работающие по протоколам HTTP и LDAP (сертификаты X.509). Центр сертификации уже входит в поставку Windows 2000 Server; в платформе .Net будет встроена поддержка цифровых сертификатов. Остается нерешенной только проблема защищенного хранения цифровых сертификатов.

- Однако даже индивидуальным пользователям к таким хранилищам стоит относиться с опаской: если специальное устройство хранит все пароли пользователя (в том числе и его private key) и впускает его в систему по аппаратному ключу, то достаточно подобрать к этому устройству один пароль — и все секреты как на ладони…