БАЗОВЫЙ ДОВЕРЕННЫЙ МОДУЛЬ "МОБИЛЬНЫЙ КЛИЕНТ"

Зорин Виталий,
канд. техн. наук, системный аналитик ОАО «ЭЛВИС-ПЛЮС»

PC Week/RE № (478) 16`2005 от 10.5.2005

Для непрерывности бизнеса под рукой постоянно должен быть рабочий инструмент. Требование мобильности подразумевает использование ноутбука вне корпоративного периметра, в среде с высоким уровнем угроз по отношению к информационным ресурсам как непосредственно компьютера, так и всей корпоративной информационной системы (КИС) в целом. Рассмотрим типы угроз при работе мобильного сотрудника с ресурсами КИС.

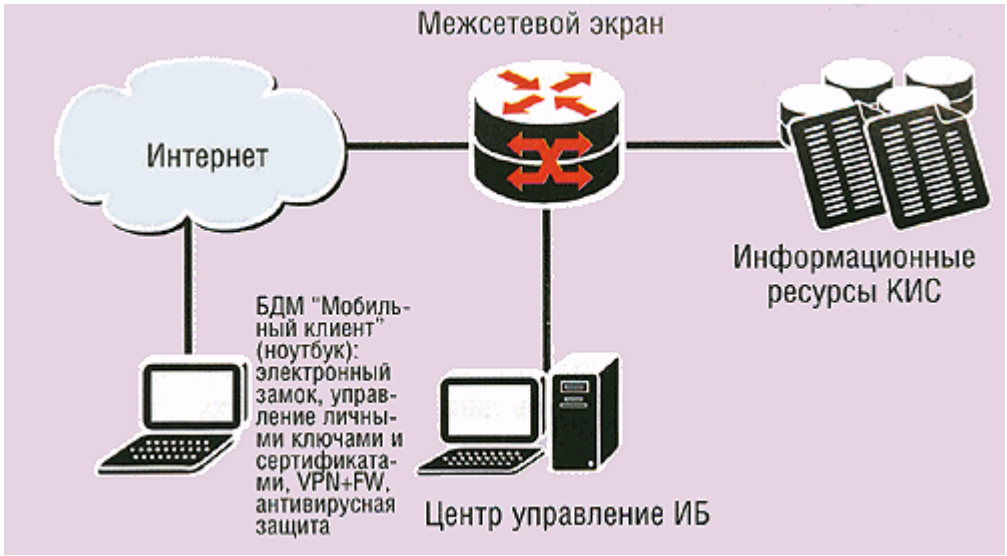
Первая группа угроз связана с кражей или потерей самого ноутбука, что случается не столь уж редко. Из-за возможности раскрытия конфиденциальной информации такая пропажа резко увеличивает риск потерь для владельца ноутбука и для организации, предоставляющей ноутбуки своим сотрудникам. При этом вероятность успешности взлома похищенного ноутбука близка к единице, так как злоумышленник имеет неограниченное время и средства для вскрытия системы защиты.

Вторая группа угроз связана с кражей аутентификационных данных, необходимых для дистанционной работы сотрудника с КИС.

Наконец, третья группа угроз - это возможность заражения компьютера вирусами, троянцами и другим вредоносным кодом при работе в Интернете.

Таким образом, для того чтобы все риски свести к минимуму, необходимо обеспечить надежную защиту мобильной рабочей станции. С точки зрения существующих подходов к обеспечению безопасности ИС надежность защиты компьютера определяется уровнем доверия к его аппаратным составляющим, программным средствам (ОС, приложения) и механизмам защиты.

Описываемый здесь базовый доверенный модуль (БДМ) "Мобильный клиент" снижает риски за счет применения новой технологии защиты, разрабатываемой в спецификациях промышленного комитета стандартов TCG (см. PC Week/RE, N 12/2005, с. 27).



Использование БДМ "Мобильный Клиент"

БДМ "Мобильный клиент" предназначен для защищенной работы сотрудников с корпоративными информационными ресурсами вне и внутри периметра КИС. При правильной корпоративной политике информационной безопасности базовым доверенным модулем может быть рабочий инструмент сотрудников, клиентов, посредников, поставщиков и прочих лиц, участвующих в бизнес-процессах организации и обладающих правом доступа к конфиденциальным информационным ресурсам.

Выбор решения

Сегодня выбор надежного решения по защите мобильных рабочих станций не является сверхсложной проблемой. Дело в том, что комитет TCG выпустил спецификацию Trusted Platform Module (TPM), на основе

которой производители ноутбуков (IBM, HP, Fujitsu, Toshiba) предлагают встроенные подсистемы безопасности с использованием специальной аппаратной части - чипов безопасности производства Atmel, National Semiconductor, Infineon, ST Microelectronics.

Нас будет интересовать встроенная подсистема безопасности IBM ESS, поставляемая вместе с ноутбуками IBM ThinkPad серий R, T и X. Несмотря на свои достоинства, эта подсистема нуждается в некоторых дополнениях, которые могли бы обеспечить полноту функций безопасности БДМ "Мобильный клиент". В частности, ей необходимы функции сетевой защиты. Для решения этой задачи был использован программный продукт "Застава-Клиент", представляющий собой управляемый FW/VPN-агент. В процессе работы по созданию БДМ "Мобильный клиент" агент был доработан до продукта "Застава-SC", который вошел в состав IBM ESS.

Архитектура решения

В состав БДМ "Мобильный клиент" входят: встроенная подсистема безопасности IBM ESS; клиентское ПО IBM CSS; FW/VPN-агент "Застава-SC" компании "Элвис-Плюс"; антивирусное ПО Norton AntiVirus корпорации Symantec.

Встроенная подсистема безопасности IBM ESS

Встроенная подсистема безопасности Embedded Security Subsystem 2.0 соответствует спецификации TPM версии 1.2 и базируется на чипе безопасности AT97SC3202 компании Atmel, который обеспечивает:

- выполнение PKI-операций над ключами и паролями, таких как шифрование-дешифрование или формирование ЭЦП;
- хранение закрытых ключей и паролей во встроенной в чип памяти EEPROM;
- создание (генерацию) ключей внутри чипа;
- поддержку функций, описанных в спецификации TPM 1.2;
- взаимодействие с центральным процессором через LPC-шину;
- аппаратную проверку уровня целостности BIOS.

Принцип работы. Работа ESS заключается в создании и следовании иерархии ключевых пар. Подсистема использует чип безопасности для генерации ключевой пары пользователя, включающей открытый и закрытый ключи. Ключевая пара предназначена для защиты любых пользовательских данных - информации на жестком диске, паролей, сертификатов и т. п. Кроме того, посредством ESS создаются ключевая пара администратора и корневая (аппаратная) ключевая пара. Корневые пары для каждого чипа и соответственно для каждой рабочей станции различны. Ключевая пара администратора может быть одной и той же для всех рабочих станций и их групп либо каждая из них может иметь свою пару.

Для сохранения и восстановления созданной иерархии ключей в случае поломки БДМ или в других нештатных ситуациях ключевая пара и пароли пользователя и администратора могут быть вынесены во внешнюю файловую систему в зашифрованном открытым корневым ключом виде. То есть по сути вся защищаемая информация зашифрована корневым ключом. Таким образом, в чипе хранится только корневой ключ и все операции с его использованием не выходят за пределы чипа, что обеспечивает полную безопасность остальных ключей (пользовательских, администратора).

FW/VPN-агент "Застава-SC"

Разработанный компанией "Элвис-плюс" продукт FW/VPN-агент "Застава-SC" использует возможности встроенной системы безопасности IBM и обеспечивает для семейства продуктов "Застава" дополнительные преимущества:

- хранилище ключей, паролей, локальной политики агента и сертификатов защищено на аппаратном уровне;
- закрытый ключ и пароль базы данных не выходят за границы чипа;
- закрытый ключ и сертификат открытого ключа пользователя доверительно привязаны к аппаратному ключу компьютера;
- пароль базы данных агента соответствует паролю пользователя, хранимому в чипе;
- операции с использованием закрытых ключей и паролей не выходят за границы чипа.

Продукт "Застава-SC" устанавливается и работает в операционных системах MS Windows 2000 и MS Windows XP.

Функциональный состав БДМ

БДМ "Мобильный клиент" обеспечивает выполнение следующих функций безопасности:

- защищенное на аппаратном уровне хранение критически важных данных;
- идентификацию и аутентификацию пользователя независимо от ОС;
- генерацию паролей в соответствии с корпоративной политикой безопасности;
- блокирование атак прямого перебора паролей (атак типа Brute-Force);
- аппаратную изолированность операций с использованием закрытых ключей;
- генерацию ключей;
- защиту файлов и каталогов;
- сетевое экранирование БДМ, управляемое корпоративной политикой;
- формирование VPN-каналов, управляемое корпоративной политикой безопасности;
- проверку целостности (BIOS, событийных протоколов и т. п.);
- антивирусную защиту.

БДМ как электронный замок

Встроенная подсистема безопасности позволяет защитить информацию как при несанкционированном доступе (НСД) извне, так и в случае кражи самого ноутбука. Главной задачей является защита информации внутри ноутбука. Во-первых, ESS предоставляет независимую от ОС собственную систему идентификации и аутентификации пользователей, которая может на начальной стадии перехватить Winlogon и взять на себя весь аутентификационный процесс. При этом пользовательский пароль не выходит за границы чипа, а специальная система, настроив политику генерации надежных паролей, запретит использование "слабых" паролей. Прямой перебор паролей, или brute-force-атака, применен быть не может, так как встроенная подсистема безопасности блокирует такие попытки, увеличивая интервалы времени между последовательными попытками ввода неправильных паролей.

ESS может дополняться модулем сканирования отпечатков пальцев, а также RFID-модулем, определяющим локализацию пользователя относительно ноутбука. Вместе с обычным токеном-идентификатором встроенная подсистема безопасности при необходимости может обеспечить многофакторную аутентификацию пользователя.

На случай кражи или потери компьютера, содержащего конфиденциальную информацию, поддерживается шифрование файловой системы на основе симметричного пользовательского ключа. Симметричный ключ для шифрования жесткого диска также находится внутри чипа - в недосягаемости для потенциального злоумышленника. Защита файловой системы осуществляется в двух режимах: "на лету" и в пользовательском режиме. Режим шифрования "на лету" устанавливается для конкретной папки, и все записываемые в нее файлы автоматически шифруются. При этом пользователю не нужно выполнять каких-либо действий. Процесс шифрования-дешифрования файловой системы "на лету" осуществляется встроенной системой безопасности, и ни приложению, ни пользователю не виден. Для приложений, обращающихся к зашифрованным файлам, не требуется специальной доработки или конфигурирования. Режим шифрования "на лету" обеспечивает защиту информации в случае потери либо кражи компьютера или жесткого диска, когда злоумышленник не может легитимно войти в систему.

Пользовательский режим требует ввода пароля (биометрики или других видов аутентификации) при дешифровании, и поэтому приложения не могут обращаться к зашифрованным файлам без предварительного их дешифрования. Данный режим обеспечивает безопасность информации, хранимой на диске, в случае НСД из сети либо когда злоумышленник смог легитимно ввести пароль или осуществить НСД к работающей системе при временном отсутствии владельца.

БДМ как сетевой замок

Для защиты БДМ "Мобильный клиент" от сетевых атак применяется управляемый персональный брандмауэр. Управляемость означает возможность его динамического конфигурирования в соответствии с требованиями корпоративной политики безопасности. В частности, при доступе в Интернет локальная политика безопасности должна блокировать возможность работы пользователя с недоверенными Web-серверами и порталами. Исходя из потенциальной опасности Интернет-среды корпоративная политика работы "Мобильного клиента" должна соответствовать принципу: запрещены соединения со всеми источниками, кроме доверенных. В группу доверенных источников могут входить не только корпоративные информационные источники внутри защищенного периметра, но и КИС бизнес-партнеров, а также любые доверенные Web-ресурсы, которые не могут быть источником атак злоумышленников.

Такая политика создается как часть корпоративного подхода с помощью центра управления (ЦУ) "Застава". После трансляции в локальные политики для всех "Мобильных клиентов" она загружается в ноутбуки сотрудников по защищенному протоколу. Данный протокол обеспечивает конфиденциальность и целостность локальной политики, причем встроенная подсистема безопасности, установленная на клиенте, позволяет надежно хранить закрытые ключи.

Локальная политика принимается, активируется и выполняется FW/VPN-агентом "Застава-SC".

VPN-соединения

Продукт "Застава-SC" как FW/VPN-агент позволяет формировать защищенные VPN-соединения с КИС посредством протокола ESP (IPSec), аутентифицировать стороны сетевого взаимодействия на основе сертификатов пользователей, хостов, групп с помощью протокола IKE, поддерживать целостность IP-пакетов по протоколу AH (IPSec). Таким образом, данный продукт поддерживает все три базовых свойства безопасности информации - конфиденциальность, целостность и доступность. Доступность определяется устойчивостью протоколов IKE/IPSec к типовым DOS/DDOS-атакам.

Продукт "Застава-SC" можно использовать как внутри КИС, так и при дистанционной работе для защиты аутентификационных данных (идентификатор пользователя, пароль), передаваемых протоколами HTTP, FTP, Telnet, IMAP, POP3, SMB либо в открытом виде, либо в виде хэша. Не составляет большого труда перехватить аутентификационные данные с помощью анализатора пакетов (сниффера).

БДМ в структуре КИС

На рисунке показана схема использования БДМ "Мобильный клиент" в составе КИС. Одним из важнейших элементов является центр управления информационной безопасностью, представленный ЦУ "Застава". С его помощью формируется корпоративная политика использования базовых доверенных модулей в корпоративной сети и в Интернете.
