КОМИТЕТ СТАНДАРТИЗАЦИИ TCG

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

PC Week/RE № (474) 12`2005 от 12.4.2005

Раздражение - мать открытия.

Карл Гольдмарк

С каждым днем технологии взлома информационных систем (ИС) становятся все изощреннее. Однако несмотря на десятки миллиардов долларов, вкладываемых каждый год в системы обеспечения безопасности информации, мы вряд ли заметим существенный прогресс в технологиях защиты, пока не будут разработаны стандарты архитектур доверенной платформы и среды.

Рассмотрим механизм проникновения в систему при ее взломе. Как правило, при атаке используются уязвимости и функциональные возможности программно-аппаратной платформы рабочих станций и серверов. Без какой-либо реакции со стороны программно-аппаратной платформы вредоносный код может разместиться на дисковом пространстве, загрузиться в оперативную память и самозапуститься. В процессе атаки с целью получения конфиденциальной информации шпионский код (spyware) встраивается в системные процессы ввода-вывода пользовательской информации для перехвата паролей, ключей, идентификаторов, содержания сообщений и документов. Вредоносный код не только считывает информацию с буфера клавиатуры и кадрового буфера видеокарты, но и эмулирует запросы на получение информации, меняет содержание памяти, а через контроллер DMA получает доступ напрямую к защищенной памяти.

Не лучше обстоят дела и с внутренними механизмами любой программно-аппаратной платформы от несанкционированного подключения внешних накопителей, разнообразных USB-устройств, принтеров и т. п. Такие механизмы просто отсутствуют!

Аналогичный пробел существует и в сетевых программно-аппаратных платформах и системах.

Отсутствие в современных ИТ-продуктах (серверах, рабочих станциях, активном сетевом оборудовании, периферии, PDA и т. п.) надежных механизмов контроля за собственной программно-аппаратной средой, а в более обобщенном виде отсутствие архитектурных и проектных решений по доверенной среде и доверенной платформе - причина незначительного прогресса технологии безопасности за последние годы.

Необходимость разработки и стандартизации решений в области архитектуры доверенной платформы и среды привела к появлению организации Trusted Computing Group (TCG). Ее миссия, согласно учредительным документам TCG, - разработка и продвижение открытых спецификаций промышленного стандарта, определяющего платформонезависимые доверенные модули и их программные интерфейсы.

По своему статусу TCG - некоммерческая международная организация, что предполагает открытое членство с тремя видами участия: учредители, спонсоры, члены. Совет директоров состоит из учредителей и членов-спонсоров. Среди учредителей основные игроки рынка: IBM, Microsoft, Intel, HP, Sun, AMD.

Устав и регламент - обычный для некоммерческой структуры.

Для публикующихся спецификаций применяется типовая промышленная патентная политика (разумная и недискриминационная).

В рамках TCG образованы рабочие группы по следующим направлениям:

- спецификация TPM чипа безопасности (Intel[1]);
- спецификация TSS программного интерфейса (IBM);
- рабочие станции PC (Intel);
- серверы (HP);

[1] Руководит работой группы представитель компании Intel.

- инфраструктура (Verisign, Intel);
- устройства хранения информации (Seagate);
- внешние устройства (Comodo);
- печатающие устройства (HP);
- мобильные телефоны (Nokia).

Активная позиция Intel в деятельности организации связана с тем, что высшим менеджментом этой компании уже давно продвигается идея встраивания функций безопасности в разрабатываемые процессоры и чипсеты. В последние годы эту инициативу Intel называет технологией La Grande, составной частью которой являются спецификации TCG.

Следует отметить, что президентом и председателем совета директоров TCG избран представитель IBM Джим Ворд. Компания уже несколько лет выпускает ноутбуки ThinkPad и рабочие станции ThinkCenter со встроенной системой безопасности и де-факто является лидером практической реализации спецификаций TPM и TSS.

К октябрю 2004 г. членами TCG являлись 82 организации, среди которых известные в мировой ИТ-индустрии поставщики аппаратного и программного обеспечения.

Спецификации, разрабатываемые TCG, направлены на создание надежной защиты критичной информации (ключей, паролей), файлов, приложений, на формирование механизмов, обеспечивающих принципиальную невозможность несанкционированного вторжения в ИС через "чужие" аппаратные и программные компоненты. С учетом заложенных в спецификации TCG механизмов контроля собственных программно-аппаратных компонентов вырисовывается возможность создания теоретически[2] неуязвимых доверенных платформ и информационных систем.

Естественно, что TCG не ставит задачей текущего дня разработку спецификации доверенной платформы или системы. Работа над спецификациями осуществляется по принципу "от простого к сложному". В данный момент завершена работа и получены первые практические результаты по спецификации TPM, определяющей программно-техническую реализацию доверенного модуля (чип безопасности), и по спецификации TSS, определяющей программный интерфейс для работы с модулем внешних приложений. В дальнейшем, по всей видимости, появятся спецификации по контролю целостности и подлинности программных компонентов, системных файлов, журналов, реестров и т.п., а также идентификации и аутентификации аппаратных компонентов доверенной платформы.

Много усилий TCG прилагает к обоснованию безопасности новых спецификаций с точки зрения неприкосновенности частной жизни. Как известно, инициативы компаний Sony и Microsoft в продвижении стандарта DRM (Digital Right Management) для лицензионной защиты мультимедиа-продукции и ПО встретили ожесточенное сопротивление гражданского общества. По аналогичной причине компании Intel не удалось на практике реализовать встроенную в процессор систему идентификации выпускаемой продукции. TCG заявляет, что все разрабатываемые ею спецификации гарантируют неприкосновенность частной жизни и обеспечивают полный контроль пользователя над системами, в которых используются спецификации TCG. В качестве примера можно привести ноутбук IBM ThinkPad с чипом безопасности, при эксплуатации которого пользователь может легко включить или выключить встроенную систему безопасности без каких-либо тяжелых последствий. Право выбора заложено и в проекте новой ОС Longhorn от компании Microsoft. Разрабатываемая операционная система будет иметь две независимые части: обычную традиционную ОС и защищенную, и пользователь по своему выбору сможет работать либо в обычной, либо в доверенной ОС.

В целом политическая позиция TCG определяется тремя утверждениями:

- спецификации TCG усиливают защиту персональной идентификационной информации;
- открытая модель позволяет любым группам разрабатывать технические и программные средства, системы, базирующиеся на спецификациях TCG;
- пользователи сохраняют свободу выбора при удовлетворении своих нужд в отношении программных и технических средств и платформ.

[2] Ошибки реализации любого теоретически абсолютно надежного решения не обеспечивают 100%-ную защиту.

TCG обязуется приложить разумные усилия, дабы обеспечить совместимость будущих спецификаций с уже существующими.

Можно констатировать, что целью спецификаций TCG являются надежная защита при контроле со стороны пользователя и соблюдение неприкосновенности частной жизни.

Работа TCG направлена не только на создание спецификаций будущих доверенных платформ и систем, но и на внедрение новой технологии безопасности в существующие ИС. Использование спецификации TPM при разработке приложений в текущий момент может обеспечить:

- аппаратную защиту ключей, используемых для обеспечения конфиденциальности и целостности информации при ее хранении на носителях (файлы, массивы, библиотеки) и передаче по сети (электронная почта, сетевой трафик);
- аппаратную защиту паролей и других аутентификационных данных, которые ранее хранились в файловой системе;
- снижение стоимости средств аппаратной защиты - в частности, можно сэкономить на приобретении и обслуживании токенов (распространение, потеря, замена), периферийных устройствах для токенов и разработке решений по их встраиванию в рабочие станции;
- неограниченную по сравнению с обычными токенами емкость хранения идентификаторов, паролей, ключей и критичных файлов.

Внедрение спецификаций TCG в новые приложения может предоставить им безопасный дистанционный доступ через совместную аутентификацию рабочей станции и пользователя, а также усиленный механизм обеспечения конфиденциальности информации за счет проверки целостности платформы перед дешифрацией данных.
