аппаратные платы шифрования — находка для шпиона

крис касперски, ака мыщъх, no-email

надежные криптосистемы — важнейшее звено любого защитного комплекса. ассортимент предлагаемых решений достаточно широк и простилается от программных пакетов до плат аппаратного шифрования, которые в глазах неспециалистов кажутся намного более стойкими уже хотя бы потому, что они "аппаратные". однако, не все "железки" одинаково полезны, более того, далеко не все "железки" полностью состоят из железа и многие из них имеют ту же самую стойкость, что и программные решения.

введение или внутри коробки

Большинство плат аппаратного шифрования конструктивно представляют собой PCI-контроллер, несущий на своем борту: а) блок управления; б) шифропроцессор; в) аппаратный датчик случайных чисел; г) микросхемы буферной памяти; д) элементы "обвязки", заставляющие все это хозяйство как-то работать.

Шифрофроцессор (которых может быть и несколько) реализует тот или иной известный и апробированный криптоалгоритм, стойкость которого не вызывает сомнений, а длина ключа исключает возможность вскрытия шифротекста путем перебора (ну, это в идеале она исключает, некоторые аппаратные платы шифрования работают с ключами длинною 40-бит или около того, что легко ломается не только правительственными организациями, но и хакерами-одиночками, особенно если они используют для перебора ключей сеть "дронов", состоящую из сотен тысяч машин, зараженных червями). Программным образом можно реализовать тот же самый алгоритм ничуть не хуже, используя мощность центрального процессора, быстродействие которого вполне достаточно даже для потокового шифрования данных "на лету" самыми тяжеловесными алгоритмами.

Аппаратный датчик случайных чисел, пожалуй, главное преимущество плат шифрования, поскольку, программно сгенерировать случайно число невозможно, а без случайных чисел нельзя создать корректную реализацию большинства популярных криптоалгоритмов. Однако, качество аппаратных датчиков варьируется в очень широких пределах. С другой стороны, на ПК даже без всяких дополнительных приспособлений можно создать надежный генератор на базе клавиатурного или мышиного ввода — просто измеряя время задержек нажатия на клавиши с точностью до сотых секунд. Многие программные шифропакеты именно так и поступают, обеспечивая надлежащий уровень качества, достающийся практически даром.

Вероятно, самым сильным аргументов в пользу аппаратных решений является их устойчивость к воздействиям со стороны вредоносного программного обеспечения. Действительно, даже если шифрование реализовано на уровне драйвера (или интегрировано в ядро операционной системы), любой другой драйвер может модифицировать защитный код по своему усмотрению, например, внедрив в него закладку, перехватывающую ключи шифрования и передающие их хакеру по скрытому каналу связи.

Считается, что аппаратные решения полностью свободны от этой угрозы. Но так ли это?

атака на железку

На отечественном рынке большой популярностью пользуется продукция компании Анкад (http://www.ancud.ru), специализирующейся на системах шифрования и выпускающая большой ассортимент аппаратных решений.

Рассмотрим, например, плату Криптон-Замок, а точнее интерфейс взаимодействия с ней, подробно описанный на сайте самой компании (http://www.ancud.ru/catalog/windk.html). От уровня приложений до портов ввода/вывода разворачивается целая иерархия, включающая в себя библиотеку CryptAPI.dll (которая, как и следует из ее названия, реализует криптографический интерфейс), и драйвер (CRYPTON.SYS — для Windows NT, CRYPTON.VXD – для Windows 9x), управляющей платой шифрования.

Допустим, злоумышленнику удалось внедрить в целевой компьютер вредоносное ПО. Что он может сделать? Первое, что приходит в голову, — это внедриться в CryptAPI.dll (или CRYPTON.SYS/CRYPTON.VXD) и перехватывать ключи шифрования. Но это еще не самое страшное! Это ведь по сути дела тривиальная утечка информации. Будет хуже, если хакер использует технику подмены ключей на лету, позволив нам зашифровать очень много данных, а затем в один "прекрасный" момент прекратит делать это. Поскольку, подлинный ключ шифрования нам неизвестен, зашифрованные данные можно считать потерянными _навсегда_ (если, конечно, их не удастся "выкупить" у хакера за приемлемую цену). Наконец, хакер может модифицировать библиотеку CryptAPI.dll таким образом, чтобы никакое шифрование вообще не выполнялась или же выполнялось тривиальное псведо-шифрование, легко вскрываемое даже без знания ключа.

В этом смысле аппаратный комплекс Криптон-Замок защищен ничуть не лучше, чем любое программное решение, только если программные решения зачастую распространяются на бесплатной основе в открытых текстах, за каждый экземпляр Криптона необходимо выложить денежки и, кроме того, аппаратные решения, в отличии от программных, подвержены внезапных отказам. Если Криптон-Замок выйдет из строя, а фирма Анкад к тому времени свернет свою деятельность — как же мы получим доступ к зашифрованным данным?!

Выходит, что платы аппаратного шифрования наследуют все недостатки программных решений, да еще добавляют к ним свои собственные? Не торопитесь в выводами! Не все так просто!

между контроллером и жестким диском

Компания Abit выпускает плату потокового аппаратного шифрования Secure IDE, врезающуюся между IDE-контроллером и жестким диском. С точки зрения операционной системы процесс шифрования протекает абсолютно прозрачно. Secure IDE не требует установки дополнительных библиотек или драйверов, а потому хакер при всем своем желании никак не может до него "дотянуться". Ни перехватить ключи шифрование, ни подменить их — программным путем невозможно в принципе, поскольку, плата реализована на 100% аппаратно и функционирует совершенно независимо от программного обеспечения.

К сожалению, Secure IDE присущ серьезный недостаток и те экземпляры, которые поставляются в Россию, используют чип X-40 от eNOVA, реализующий нестойкое 40-битное шифрование. Чипы, реализующие 128-шифрование, компания Abit посчитала слишком дорогим решением для массового рынка, однако, фирма Анкад выпускает комплексы КРИПТОН-IDE и КРИПТОН-SATA, полностью идентичные Secure IDE, только использующие криптостойкий алгоритм ГОСТ 28147-89. Принцип, лежащий в их основе, все тот же — врезаемся между контроллером и жестким диском, шифруя данные "на лету" в полностью автономном режиме, без установки какого бы то ни было программного обеспечения, подверженного компрометации.

заключение

Аппаратные платы, предоставляющие программному обеспечению набор функций для шифрования, имеют ту же самую стойкость, что и чисто программные решения, поскольку, интерфейс между платой и операционной системой — самое слабое звено, легко расщепляемое хакером. Полностью аппаратные платы, работающие в автономном режиме, уже не могут быть скомпрометированы программным путем. Но длина ключа шифрования и быстродействие зачастую существенно уступает их программным аналогам, а потому вопрос: что лучше, а что хуже остается открыт…

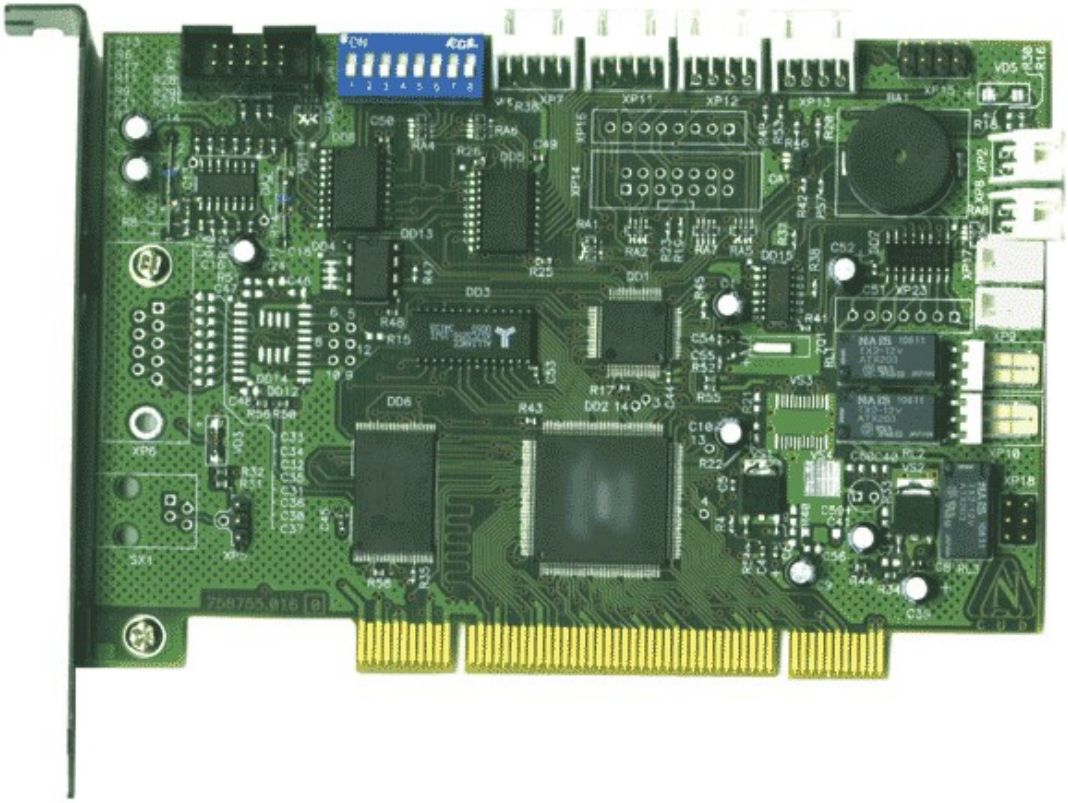

Рисунок 1 внешний вид платы Криптон-Замок

Рисунок 2 внешний вид платы Secure-IDE

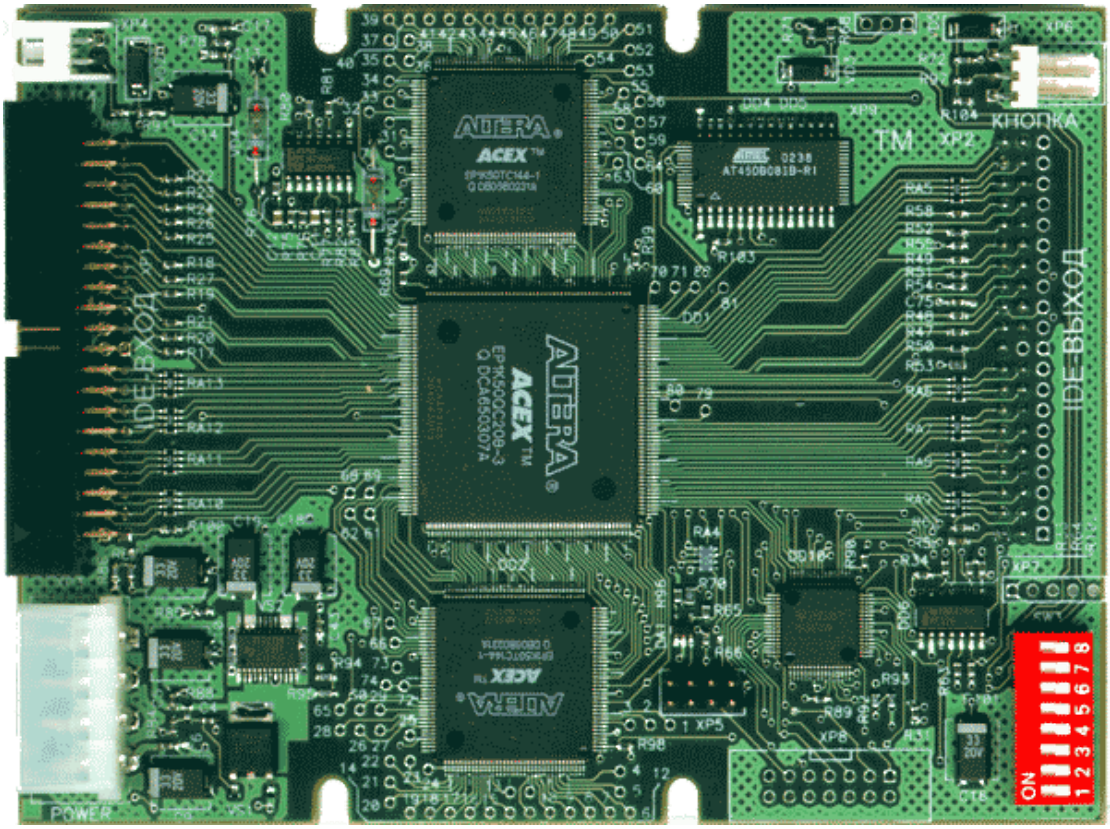

Рисунок 3 внешний вид платы Криптон-IDE