USB FLASH плюс аппаратное шифрование — взгляд очевидца

крис касперски, no-email

занимаясь восстановлением данных с различных накопителей, автор долгое время отказывался ковырять зашифрованные FLASH-накопители с утерянными паролями, считая это пустой тратой времени, пока однажды с удивлением не обнаружил, что во многих случаях поддержка аппаратного шифрования, заявленная производителем, представляет собой сплошную фикцию! вот так чертик из табакерки!

введение в тему

FLASH-накопители активно используются для хранения данных и переноса их между компьютерами, что ребром ставит вопрос о безопасности. FLASH-накопители часто становятся объектом кражи. Их легко потерять. Их содержимое легко прочитать, внедрив вредоносное программное обеспечение на наименее защищенный компьютер, с которым "флешке" приходится общаться, причем, прочесть (на логическом уровне) можно в том числе удаленные, но еще физически не затертые файлы, среди которых нередко попадаются и конфиденциальные.

Количество утечек информации, в которых так или иначе замешаны "флешки" неуклонно растет и пресса буквально кишит ужасными историями, пугающими корпоративных пользователей для успокоения которых производители предлагают FLASH-накопители с поддержкой функций аппаратного шифрования. Вот, например, Kingston DataTraveler Secure/ Secure Privacy Edition, облаченные в титановое покрытие и сохраняющие работоспособность при погружении в виду до 1,2 метров, смотрятся очень стильно. И для пущей защищенности поддерживают 256-битное аппаратное AES-шифрование, управляемое программным обеспечением MyDataZone, работающим под Windows.

U-turn или полный разворот

Стоп! Какое такое программное обеспечение, если функция шифрования аппаратная?! Мало того, что его нужно ставить на каждый компьютер, участвующий в обмене данных (а что делать, если владелец компьютера категорически против такого расклада?!) мало того, что обозначенное программное обеспечение, записанное на "флешке", подвержено вирусному заражению, так в довершении всего, как уже говорилось в соседней статье про платы шифрования, хакеру ничего не стоит внедрить закладку, крадущую пароли и тогда шифрование потеряет весь смысл! (Кстати, в технической документации на Kingston DataTraveler Secure шифрование обозначено как программно-аппаратное, то есть, Kingston как известный производитель, не может позволить себе нагло лгать, правда, к отделу маркетинга это уже, увы, не относится).

И хотя ходят слухи про существование "флешек" с поддержкой био-идентификации на основе отпечатков пальцев, которые не требуют установки дополнительного программного обеспечения, а потому и не подвластны для малвари, сам автор таких штучек никогда не видел, но отчетливо представляет себе их стоимость, простилающуюся дальше орбиты Марса, в то время как программные средства шифрования (типа RAR'a) либо вообще бесплатны, либо стоят чуть дороже бутылки пива, причем за их надежность можно поручиться если не головой, то хотя бы дать палец на отсечение.

гадание на кофейной гуще

Не собираясь заниматься (анти)рекламой, автор не будет перечислять производителей, заявляющих о поддержке функций аппаратного шифрования, но никак не реализующих их на практике. Опасаюсь быть побитым. Откуда мне, простому кодокопателю, знать: то ли это происки хитрых китайцев, клепающих в подвале поддельные "флешки", и упрощающие их до безобразия путем выкидывая всех "лишние" деталей, то ли, действительно, производители выдают желаемое за действительное, то ли еще какие причины…

Конечному потребителю все эти разборки сугубо перпендикулярны. Его интересует качество шифрования. А шифрование в строгом смысле этого слова к потребительским

характеристикам не относится. Это уже внутренние аспекты реализации, оценить параметры которых по силу только специалистам. Даже если электронщик разберет FLASH-накопитель, вытащит чип памяти и прочитает его содержимое — ну и что с того? Допустим, данные _выглядят_ зашифрованными. Но означает ли это, что они действительно _надежно_ зашифрованы?! Ответ могут дать только криптоаналетики после годов упорного труда. Причем, анализировать необходимо _каждый_ экземпляр FLASH-накопителя, поскольку, "подпольщикам" ничего не стоит подделать чужую продукцию, и продать ее нечестным на руку дилерам, подмешивающих ее в оригинальные партии.

Пользуясь аппаратными средствами, вы всегда рискуете. Нет никаких гарантий, что шифрование действительно выполнено надежно. Лично автор неоднократно сталкивался с тем, что все шифрование сводится к тому, что во FLESH-накопитель устанавливается дополнительный чип, проверяющий пароль и в случае успеха, открывающий доступ к данным. Сами данные при этом остаются _вообще_ незашифрованными!!! Естественно, программным путем подобрать пароль невозможно, т. к. чип вводит длительные задержки во времени после каждой неверной попытки, достигающие десятков секунд. Однако, если "флешка" находится в наших руках — достаточно разобрать ее, выкинуть защитный чип и спокойно считать все данные.

Короче говоря, аппаратное шифрование — это рулетка, даже еще хуже. В рулетке по крайней мере можно выиграть… А вот в шифровании… даже если модуль шифрования реализован правильно, он все равно нуждается в управляющем программном обеспечении, нивелирующим все достоинства аппаратного решения.

шифрование — своими руками

Если вы действительно заботитесь о безопасности — либо используйте "прозрачные" платы шифрования, вставляемые между FLASH-накопителем и USB-портом от известной компании, продукции которой можно доверять, либо же чисто программные пакеты, апробированные и одобренные криптоаналетиками.

В частности, архиватор RAR, встречающийся повсеместно от Windows до Linux, использует очень надежный алгоритм шифрования и что самое главное — он проверяет не контрольную сумму ключа (как это делают многие его конкуренты), а контрольную сумму распакованного и расшифрованного этим ключом файла. Поскольку, распаковка требует времени, то даже на самых быстрых машинах скорость перебора не достигает и тысячи паролей в секунду, а офисные компьютеры выдают максимум сотни. Для сравнения — "ломалки" для pkzip'a за это же время перебирают до миллиона ключей.

Поскольку, программное обеспечение для шифрования хранится не на флешке, а на компьютере, то исчезает опасность вирусного заражения (если, конечно, на самой флешке не записано никаких файлов, которые могут служить средой обитания для зловредных программ). Перехватить пароли или модифицировать код шифрующей программы так, чтобы она всего лишь имитировала шифрование, не выполняя его в действительности, технически возможно, но практически очень сложно, особенно, если хакер не знает какое именно программное обеспечение используется жертвой. К тому же жертва сегодня может использовать RAR, завтра — 7zip, а послезавтра что-нибудь еще. Многообразие версий серьезно затрудняет атаку, поскольку не допускает универсальных сценариев нападения. Напротив, программное обеспечения для управления модулями аппаратного шифрованием, довольно хорошо предсказуемо и количество всевозможных версий скорее мало, чем велико, а потому хакеру не так уж и трудно написать атакующую утилиту, поддерживающую весь спектр оборудования.

Вывод — аппаратное шифрование во FLASH-чипах это никакого не шифрование, а полная профанация, от которой больше вреда, чем пользы. И дело даже не в потраченных деньгах, а в расплате за иллюзию безопасности.

Рисунок 1 FLASH-накопитель Kingston DataTraveler Secure с поддержкой программно-аппаратного шифрования данных

Рисунок 2 FLASH-накопитель Kingston DataTraveler Elite с поддержкой программно-аппаратного шифрования данных