Дробинина Александра Викторовна
студентка
Логинов Вячеслав Сергеевич
студент
Кротова Елена Львовна
канд. физ.-мат. наук, доцент
ФГБОУ ВПО «Пермский национальный
исследовательский политехнический университет»
г. Пермь, Пермский край

ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ BITLOCKER

***Аннотация**: в рамках данной статьи рассмотрена защита диска с помощью встроенной программы BitLocker (BitLocker Drive Encryption), а также шифрование тома, принципы шифрования и проверка целостности.*

***Ключевые слова**: защита диска, BitLocker, шифрование тома, проверка целостности.*

Технология BitLocker выполняет две взаимодополняющие, но различные функции:

1. Шифрование всего тома ОС Windows®.

2. Проверка целостности загрузочных компонентов ОС на компьютерах с совместимым доверенным платформенным модулем (TPM).

Также BitLocker поддерживает многофакторную проверку подлинности для дисков операционной системы. Для этого требуются совместимые версии TPM (1.2 или 2.0) и BIOS, поддерживающая TPM и статический корень измерения доверия (Static Root of Trust Measurement), определенный в спецификациях TCG. Далее более подробно рассмотрим функции и принцип шифрования.

Полное шифрование тома. Шифрованию подлежит том, а не физический диск. При этом том может занимать часть диска, включать диск целиком, а может состоять их массива нескольких дисков.

При этом необходимо учитывать, что жесткий диск должен быть разбит хотя бы на два диска:

1. Диск операционной системы (или загрузочный диск), который содержит операционную систему и файлы, необходимые для ее работы, должен быть отформатирован в файловой системе NTFS.

2. Системный диск, содержащий файлы, необходимые для загрузки Windows после того, как BIOS загрузит платформу. Для этого диска шифрование BitLocker не включается. Для работы шифрования BitLocker системный диск не должен быть зашифрован, он не должен являться томом операционной системы и должен быть отформатирован в файловой системе NTFS. Емкость системного диска должна быть не менее 1,5 гигабайт (ГБ).

Начиная с Windows Vista SP1 появилась возможность шифровать несистемные тома. После создания разделов необходимо инициализировать TPM-модуль в ПК, где он есть, и активировать BitLocker. В Windows 7 появился BitLocker To Go, позволяющий шифровать сменные носители, а также снижены требования для загрузочной части, для неё достаточно 100 Мб. При установке Windows 7 на пустой диск загрузочный раздел создаётся автоматически.

Принцип шифрования. BitLocker использует алгоритм AES, всего доступно 4 вариации в зависимости от настроенной длины ключа:

– AES 128;

– AES 128 с Elephant diffuser (используется по умолчанию);

– AES 256;

– AES 256 с Elephant diffuser.

Выбраный том шифруются ключом шифрования всего тома (full-volume encryption key, FVEK). Затем ключ FVEK шифруется основным ключом тома (volume master key, VMK).

Ключ FVEK в зашифрованном виде хранится на диске среди метаданных тома. При этом он никогда не попадает на диск в расшифрованном виде.

Ключ VMK тоже шифруется, или «охраняется», одним или несколькими предохранителями ключей. Предохранитель по умолчанию – TPM. Пароль восстановления тоже создается как предохранитель на случай экстренных ситуаций.

В случае отсутствия совместимого TPMили BIOS, система потребует от пользователя вставлять USB-ключ запуска, чтобы запустить компьютер или вывести его из спящего режима. Данный вариант не обеспечивает проверку целостности системы перед запуском, предоставляемую шифрованием BitLocker с доверенным платформенным модулем.

Можно повысить защищенность за счёт двухфакторной проверки подлинности, для этого объединив TPM с числовым ПИН-кодом или с частичным ключом, хранимым на USB-накопителе.

BitLocker можно отключить, не расшифровывая данные. В этом случае ключ VMK защищается только новым предохранителем ключа, который хранится в незашифрованном виде. Этот ключ позволяет системе получать доступ к диску так, словно он не зашифрован.

При запуске система ищет подходящий предохранитель ключа, опрашивая TPM, проверяя порты USB или, если необходимо, запрашивая пользователя (что называется восстановлением). Обнаружение предохранителя ключа позволяет Windows расшифровать ключ VMK, которым расшифровывается ключ FVEK, которым расшифровываются данные на диске. Весь процесс показан на рис. 1.

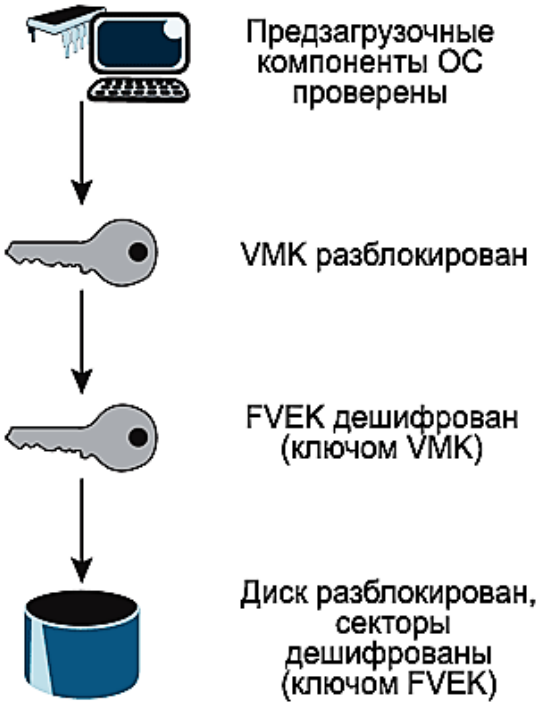

Рис. 1. Процесс запуска BitLocker по умолчанию

Проверка целостности. Поскольку компоненты, выполняющие начальную стадию загрузки, должны оставаться незашифрованными (иначе компьютер не сможет запуститься), злоумышленник может изменить их код (создать rootkit) и так получить доступ к компьютеру, даже если данные на диске останутся зашифрованными, что открывает доступ к конфиденциальной информации, например, ключам BitLocker или паролям пользователей, которые могут быть использованы для обхода других средств защиты.

Шифрование BitLocker может использовать доверенный платформенный модуль для проверки целостности компонентов загрузки и данных конфигурации загрузки. Это помогает гарантировать, что при использовании шифрования BitLocker шифрованный диск будет доступен, только если эти компоненты не были подменены и шифрованный диск установлен в исходном компьютере.

Шифрование BitLocker помогает гарантировать целостность процесса запуска с помощью следующих действий:

1. Обеспечение способа проверки целостности корневого файла и файлов, используемых на ранних этапах загрузки, и гарантирование отсутствия враждеб-

ных изменений в этих файлах, которые могли быть выполнены, например, вирусами загрузочных секторов или средствами редактирования компонентов загрузки.

2. Улучшенная защита, противостоящая программным атакам, когда компьютер находится вне сети. Любое альтернативное программное обеспечение, которое может запустить систему, не получит доступ к ключам шифрования для диска операционной системы Windows.

3. Блокировка системы при замене файла. Если любой из контролируемых файлов был заменен, система не запустится. Это предупредит пользователя о замене, так как система не сможет быть запущена в обычном порядке. В случае блокировки системы шифрование BitLocker обеспечит простой процесс восстановления.

Хотя проверка целостности не гарантирует абсолютную защиту, этого достаточно, чтобы значительно усложнить задачу вероятному злоумышленнику и предотвратить ряд угроз.

Резюмируя, можно отметить, что BitLocker возможно использовать как инструмент обеспечения защиты данных от нежелательного ознакомления. К его несомненным плюсам можно отнести: возможность более детальной настройки под свои нужды, шифрование томов, сравнительно низкое снижение производительности дисков, а также выбор способа защиты ключа. К недостаткам же можно отнести: необходимость совместимого TPM и BIOS для полноценной работы, ограничение на дисковое пространство, вероятность потерять данные в случае утраты ключа, уязвимость перед некоторыми угрозами.

Таким образом можно сделать вывод, что одного лишь шифрования для полноценной защиты недостаточно, а само его применение не всегда оправдано. Именно поэтому, прежде чем использовать BitLocker, стоит определить необходимость его использования.

Список литературы

1. Библиотека всемирно известных изданий // Информационный центр; ред. microsoft.; Web-мастер microsoft [Электронный ресурс]. – Режим доступа: https://technet.microsoft.com/ru-ru/library/cc732774(v=ws.11).aspx

2. Байрон Хайнз. Защита данных с помощью шифрования диска BitLocker [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/analytics/296866.php (дата обращения: 14.05.2016).