Васильева И.Н. Надежность шифрования – взгляд с точки зрения форензики// Конвергенция цифровых и материальных миров: экономика, технологии, образование: сборник научных статей международной научно-практической конференции, 21-22 июня 2018 г., Санкт-Петербург / под ред. В.В.Трофимова, В.Ф.Минакова. – СПб.: Изд-во СПбГЭУ, 2018. – С.215-220.

Васильева И.Н., к. ф.-м. н., доцент СПбГЭУ,
доцент СПб университета МВД России, Санкт-Петербург

НАДЕЖНОСТЬ ШИФРОВАНИЯ – ВЗГЛЯД С ТОЧКИ ЗРЕНИЯ ФОРЕНЗИКИ

Аннотация. Рассмотрены способы и инструменты криптографической защиты информации в компьютерных системах. Обсуждается проблема надежности реализации шифрования и возможность доступа к защищенным данным с помощью инструментов компьютерной криминалистики. Рассмотрены основные подходы к извлечению исходной информации для вскрытия зашифрованных данных.

Ключевые слова: шифрование, криптографическая защита, парольная защита, форензика, компьютерная криминалистика

Vasilyeva I. N., vice professor, St. Petersburg State University of Economics,
St. Petersburg University of MIA of Russia, St. Petersburg

RELIABILITY OF ENCRYPTION TOOLS – THE FORENSICS POINT OF VIEW

Annotation. Methods and instruments of cryptography information security in computer systems are considered. The problem of reliability of implementation of encryption tools and a possibility of access to the protected data with the help of computer forensics tools is discussed. The main approaches to extraction of the initial information for the encrypted data analysis are considered.

Key words: encryption, cryptographic protection, password protection, forensic, computer forensics

Как известно, используемые современные криптографические алгоритмы, такие как AES, 3DES, отечественные ГОСТ Р 34.12–2015 «Кузнечик» и «Магма», обладают достаточной вычислительной стойкостью. Большие длины ключей (от 128 бит) исключают практическую возможность вскрытия методом подбора ключа. Вместе с тем, успешные атаки на зашифрованную информацию обусловлены, прежде всего, уязвимостями реализаций средств криптографической защиты информации (СКЗИ). При исследовании надежности СКЗИ представляет интерес взгляд с точки зрения форензики – компьютерной криминалистики, нацеленной на поиск и извлечение информации (доказательств) из компьютерных систем.

Требования безопасности приложений приводят к тому, что все больше данных на компьютере хранится в зашифрованном виде. Так, например, популярные браузеры сохраняют данные учетных записей пользователей (логины и пароли) для доступа к сайтам, сессии и файлы cookies, служащие источником личной информации. Вместе с тем, такая информация по большей части зашифрована. Для защиты данных браузеры Chrome и Edge (IE) в

операционной системе Windows используют интерфейс DPAPI (Data Protection API), позволяющий реализовать функции шифрования и расшифрования как данных, так и памяти. При этом, как правило, ключ шифрования генерируется на основе пользовательского пароля, используемого для входа в Windows. Механизмы DPAPI не обеспечивают абсолютно надежной защиты, что подтверждается опытом использования криминалистического программного обеспечения, например, Belcasoft Evidence Center.

Еще один пример – хранение синхронизированных данных и резервных копий информации с устройств, работающих под управлением операционных систем Android, iOS и Windows 10 в облачных хранилищах: Google Account, iCloud и Microsoft Account соответственно. Полученные с устройства облачные данные в ряде случаев никак не контролируются пользователем и могут содержать пароли, ключи доступа к зашифрованным томам, а также личную информацию (переписку, контакты, данные о звонках, геолокационные данные и прочее). Извлечение таких данных позволяет получить доступ к другим устройствам и хранилищам. Однако сама процедура извлечения данных из облака является нетривиальной, поскольку разработчики используют шифрование, причем некоторые данные, например, пароли в резервных копиях, дополнительно шифруются аппаратным ключом, другие допускают обращения только с доверенного устройства. Вместе с тем, существуют криминалистические инструменты, с успехом справляющиеся с данной задачей, например, Elcomsoft Cloud Explorer, Elcomsoft Phone Breaker.

Для шифрования хранимых данных пользователем могут быть использованы встроенные криптографические функции, доступные в операционных системах Windows [1] и предназначенные для локального шифрования объектов файловой системы (EFS, Encrypting File System) и дисков (BitLocker, BitLocker Drive Encryption).

EFS фактически является надстройкой над файловой системой NTFS, позволяющей обеспечить защиту данных как во время работы ОС, так и в автономном режиме (при прямом физическом доступе к диску, с другого экземпляра ОС). Вместе с тем, EFS имеет существенные ограничения: не могут быть зашифрованы данные на разделе, отличном от NTFS (например, при копировании файла на флэш-накопитель); не могут быть зашифрованы системные файлы и области, что оставляет уязвимыми критичные данные ОС (например, такие как реестр).

Для защиты от автономных атак Microsoft предлагает использовать шифрование на уровне тома с помощью инструмента BitLocker, доступного в версиях Windows Server и десктопных версиях Enterprise и Ultimate. Для съемных носителей (томов с файловой системой, отличной от NTFS) используется технология BitLocker To Go. BitLocker ориентирован, прежде всего, на совместное использование с аппаратным криптографическим сопроцессором –

доверенным платформенным модулем (Trusted Platform Module, TPM) и глубоко привязан к конфигурации компьютера. Из-за импортных ограничений TPM на территории России недоступен, однако возможно использование шифрования BitLocker с ключом запуска, записанным на USB-накопитель. Несмотря на глубокую аппаратную привязку, шифрование BitLocker рассчитано лишь на автономные атаки при выключенной ОС. После загрузки операционной системы с использованием ключевого носителя ключи шифрования хранятся в оперативной памяти компьютера в открытом виде. Это значит, что сняв образ оперативной памяти, можно в дальнейшем получить доступ к зашифрованному тому.

Дампы оперативной памяти, а также содержание файлов гибернации и подкачки, являются основным источником данных для извлечения паролей и ключевой информации. Анализ «вовремя» снятого образа оперативной памяти позволяет получить необходимые данные для дальнейшего дешифрования пользовательских данных. Подобный анализ и дешифрование могут быть реализованы с помощью таких криминалистических утилит, как Passware Kit Forensic, Elcomsoft Forensic Disk Decryptor (доступ к содержимому дисков, зашифрованных с помощью таких известных утилит, как BitLocker, TrueCrypt, PGP, FileVault 2), Elcomsoft Advanced EFS Data Recovery, Elcomsoft Advanced Office Password Recovery, Elcomsoft Advanced PDF Password Recovery.

Решению задачи дешифрования способствует практика формирования ключей шифрования на основе пользовательского пароля – как правило, это пароль учетной записи пользователя для входа в операционную систему. Например, при хранении в Windows закрытый ключ сертификата EFS шифруется с помощью хэша пользовательского пароля. Таким образом, фактическая безопасность этих систем, в конечном счете, определяется надежностью пароля пользователя. Даже если пароль был задан специально, в ряде случаев при наличии личной информации пользователя он может быть найден с высокой вероятностью, поскольку пользователи, как правило, используют не более трех различных паролей и их модификации.

Компании, работающие на рынке криминалистического программного обеспечения, предлагают утилиты для подбора паролей, такие, как Passware Kit Forensic, Elcomsoft Distributed Password Recovery. Повышение эффективности перебора достигается распараллеливанием вычислений за счет распределения их между различными устройствами (использование мультиагентных систем), использования мощных вычислительных систем с многоядерными (например, 32-ядерных) центральными процессорами (CPU), активного использования графических процессоров (GPU) видеокарт. Современные графические адаптеры могут иметь до нескольких тысяч процессоров, что позволяет проводить эффективные параллельные вычисления. При этом скорость подбора паролей может существенно варьироваться в зависимости от используемых форматов

файлов данных, поскольку некоторые из них требуют значительной предварительной обработки традиционным способом, загружая центральный процессор.

Тем не менее, подбор пароля методом грубой силы практически неосуществим, поскольку используемые функции формирования ключа (например, PBKDF2, Password-Based Key Derivation Function), используют многократные итерации хэширования с подмешиванием случайных данных, что значительно замедляет вычисление ключа и, как следствие, существенно снижает скорость опробования паролей. Примером является процедура вычисления ключа, используемая при парольной защите документов Microsoft Office [2] – рисунок 1.

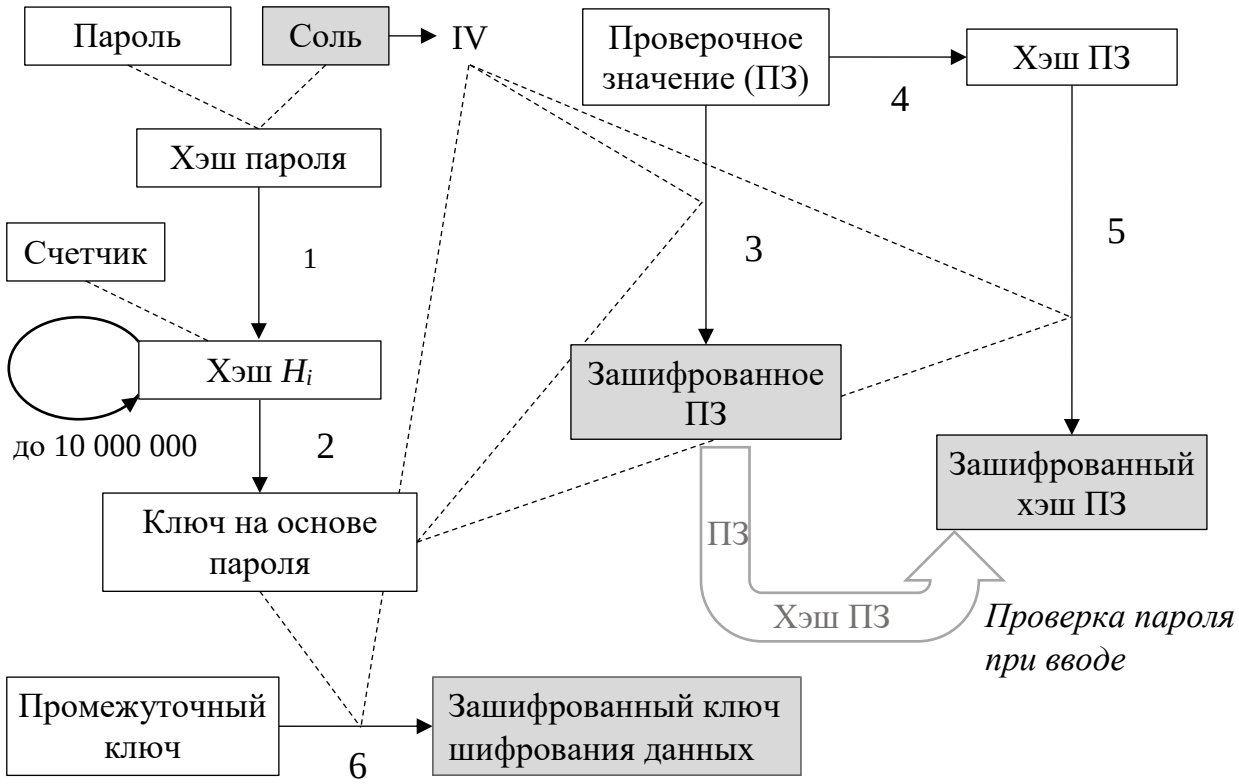

Рисунок 1. Генерация ключевой информации в документах Microsoft Office

Как видно, современные версии парольной защиты Microsoft Office допускают использование для получения ключа до 10 млн. таких итераций (конкретное число итераций настраивается с помощью групповой политики безопасности). Рекомендованные параметры функции формирования ключа для российских СКЗИ приведены в [3].

Решением является подбор пароля с помощью словаря, при этом словарь должен формироваться для пользователя индивидуально, с использованием

доступной персональной информации – ключевой информации, полученной на основе дампа оперативной памяти, файлов гибернации и подкачки; паролей, сохраненных браузерами и в реестре; другой доступной личной информации, извлеченной из различных пользовательских устройств и хранилищ – чатов, облаков, документов на диске, почтовых сообщений. При этом следует начинать с анализа файлов с наименее надежным типом шифрования. Такой подход позволяет существенно повысить эффективность вскрытия защищенных данных.

Литература

1. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. 6-е изд. Основные подсистемы ОС. – СПб.: Питер, 2014. – 672 с.
2. Защита информации в компьютерных системах: монография; под ред. Е.В. Стельмашонок, И.Н. Васильевой – СПб.: Изд-во СПбГЭУ, 2017. – 163 с.
3. Р 50.1.111–2016 «Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации» – М.: Стандартинформ, 2016. – 12 с.