Васильева И.Н. Вопросы практической надежности криптографических средств защиты информации // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 / СПОИСУ. – СПб., 2018. – С.186-189. http://spoisu.ru/files/riib/riib_5_2018.pdf

УДК 004.056.5

ВОПРОСЫ ПРАКТИЧЕСКОЙ НАДЕЖНОСТИ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Васильева Ирина Николаевна
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. летчика Пилютова, д. 1,
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, д. 21

Аннотация: В статье рассмотрены популярные средства 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 информации, парольная защита, форензика, компьютерная криминалистика

THE PRACTICAL RELIABILITY OF CRYPTOGRAPHIC PROTECTION TOOLS

Vasilyeva Irina
The St. Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, st. pilot Pilutov, 1,
The St. Petersburg State Economic University,
Russia, St. Petersburg, st. Sadovaya, 21

Abstract: The article deals with the popular cryptographic protection tools in computer systems. The problem of reliability of encryption implementation and the possibility of access to protected data using computer forensics tools are discussed. The main approaches to the extraction of initial information for the encrypted data analysis are considered.

Keywords: encryption, cryptographic protection of information, password protection, forensic, computer forensics

Введение. Большинство современных компьютерных систем, таких как операционные системы (ОС), web-серверы и СУБД, обладают встроенными средствами криптографической защиты информации (СКЗИ) для надежного хранения или защищенной передачи данных. В качестве примеров подобных средств можно привести функции шифрования файлов и папок Encryption File System (EFS) или средство шифрования диска BitLocker в операционных системах семейства Windows. При этом большинство пользователей уверено, что применяемые средства защиты обладают абсолютной надежностью за счет реализации

стойких криптографических алгоритмов, таких как AES или отечественные криптоалгоритмы ГОСТ. Как правило, большое внимание уделяется выбору длины ключа алгоритма шифрования, например, даются рекомендации использовать алгоритм AES с длиной ключа 256 бит (AES-256) вместо AES-128.

Действительно, 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 полного перебора значений ключа. Вместе с тем, успешные атаки на зашифрованную информацию в ряде случаев все же возможны и обусловлены, прежде всего, непониманием особенностей, а иногда и уязвимостями реализации СКЗИ. Поэтому при исследовании вопроса практической надежности криптографических средств представляет интерес взгляд с точки зрения форензики – компьютерной криминалистики, нацеленной на поиск и извлечение информации (доказательств) из компьютерных систем. Целью настоящей статьи является анализ популярных СКЗИ, доступных пользователям операционных систем Windows и мобильных систем.

Требования безопасности приложений приводят к широкому использованию шифрования, которое зачастую осуществляется приложением автоматически, прозрачно для пользователя и не требует, а иногда и не допускает пользовательской настройки параметров. Так, например, популярные браузеры сохраняют данные учетных записей пользователей (логины и пароли) для доступа к сайтам, сессии и файлы cookies, служащие источником личной информации, в зашифрованном виде. 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 [1].

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 [2].

Для шифрования хранимых данных пользователем могут быть использованы встроенные СКЗИ, доступные в операционных системах Windows [3] и предназначенные для локального шифрования объектов файловой системы (EFS) и дисков (BitLocker, BitLocker Drive Encryption, BitLocker To Go). 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 неактивной (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.

Снятие дампа оперативной памяти в ОС Windows не составляет большого труда, если пользователь не использует блокировку компьютера. Для этих целей могут быть использованы как встроенные механизмы самой ОС Windows, так и бесплатные утилиты, такие как Belkasoft Live RAM Capturer [4], или специальный Live-дистрибутив ОС linux (например, Ubuntu CyberPack). Такие средства загружаются в оперативную память атакуемого компьютера и, вообще говоря, изменяют ее содержимое, однако занимают, как правило, очень немного места, что позволяет их использовать в криминалистической практике. В более сложном случае (если невозможен запуск программного обеспечения на атакуемом компьютере) криминалистами может быть получен непосредственный доступ к памяти с помощью специальных плат расширения, через порт FireWire, или посредством физического изъятии оперативного запоминающего устройства с за-

мораживанием. После получения снимка оперативной памяти возможно извлечение ключей BitLocker и получение доступа к зашифрованному диску с помощью утилиты Elcomsoft Forensic Disk Decryptor. Другой путь получения доступа к данным – использование копий ключей из облачного хранилища учетной записи Microsoft или хранилищ Active Directory, либо сохраненного пользователем ключа восстановления [4].

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 [5], 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 и др.

Решению задачи дешифрования способствует и 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 известной личной информации он может быть найден с высокой вероятностью, поскольку пользователи, как правило, используют легко запоминаемые, а значит, несложные пароли [6].

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 функции формирования ключа по паролю используют многократные итерации хэширования с подмешиванием случайных данных, что значительно замедляет вычисление ключа и, как следствие, существенно снижает

скорость опробования паролей. Например, процедура вычисления ключа, используемая при парольной защите документов Microsoft Office [7, С.80-81], допускает до 10 млн. итераций хэширования. Словарная атака с использование универсальных словарей, например, орфографического, либо словарей, предоставляемых разработчиками криминалистических средств (тем же Passware), также зачастую оказывается неэффективной. Однако ситуация не является безвыходной. Решение, как это часто бывает, обусловлено наличием «человеческого фактора».

Как правило, пользователь использует не более трех различных паролей и их незначительные модификации (изменение регистра символов, замена отдельных букв на цифры или символы, добавление цифровой комбинации в начало/конец слова) для доступа к различным ресурсам. Это дает возможность реализации словарной атаки, эффективность которой существенно зависит от релевантности используемого для подбора словаря.

Общие рекомендации для криминалистов состоят в том, чтобы попытаться по возможности извлечь данные из всех устройств и облачных хранилищ, начиная с наиболее доступных, таких как данные браузеров, системные ресурсы (например, реестр Windows), файлы с наименее надежным типом шифрования. Извлеченная информация может быть использована для составления таргетированного словаря, ориентированного на конкретного пользователя. Результаты анализа снимков оперативной памяти, наряду с данными, полученными из хранилищ веб-браузеров и учетных записей почтовых клиентов могут быть использованы для создания такого словаря. Кроме того, извлеченная информация может дать представление о предпочтениях пользователя, в частности, о типе мутаций паролей, которые он, возможно, использовал. Современные средства вскрытия паролей, например, Passware Kit Forensic, Elcomsoft Distributed Password Recovery позволяют задавать определенные мутации при использовании словарной атаки. Подбор пароля с использованием таргетированного словаря, как правило, приводит к успешному вскрытию защищенной информации [8].

Заключение. Широкая распространенность и доступность современных СКЗИ может создать у неспециалиста ложную уверенность в безопасности защищаемой информации. Использование стойких криптоалгоритмов само по себе не может гарантировать высокую надежность СКЗИ, при этом дополнительная настройка таких средств, включая увеличение длины используемых ключей шифрования, не играет первостепенной роли. Более важным является четкое понимание назначения, особенностей реализации и существующих ограничений того или иного СКЗИ, а также комплексное применение защитных мер и средств (например, обязательное включение блокировки Windows при использовании средства BitLocker). Подобные условия применения СКЗИ могут быть учтены специалистами при разработке политик безопасности. Особо стоит отметить

тщательный выбор паролей, используемых при защите критически важной информации. Только комплексный подход и строгое следование политикам безопасности может гарантировать необходимый уровень защищенности данных.

СПИСОК ЛИТЕРАТУРЫ

1. Belcasoft. Forensics made easier: [сайт]. URL: https://belkasoft.com/ru/ (дата обращения: 20.09.2018).
2. Перебор паролей, восстановление доступа, расшифровка информации, мобильная криминалистика/ Elcomsoft Co.Ltd.: [сайт]. URL: https://www.elcomsoft.ru/ (дата обращения: 20.09.2018).
3. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. 6-е изд. Основные подсистемы ОС. – СПб.: Питер, 2014. – 672 с.
4. Возможен ли взлом Bitlocker? URL: http://www.spy-soft.net/vzlom-bitlocker/ (дата обращения: 20.09.2018).
5. Windows Password Recovery tools by Passware: [сайт]. URL: https://www.passware.com (дата обращения: 20.09.2018).
6. Афонин О. Использование утечек паролей для ускорения атак. 16.02.2017. URL: https://blog.elcomsoft.com/ru/2017/02/ispolzovanie-utechek-paroley-dlya-uskoreniya-atak/ (дата обращения: 20.09.2018).
7. Защита информации в компьютерных системах: монография; под ред. Е.В. Стельмашонок, И.Н. Васильевой – СПб.: Изд-во СПбГЭУ, 2017. – 163 с.
8. Афонин О. Как вскрыть до 70% паролей за несколько минут. 14.02.2017. URL: https://blog.elcomsoft.com/ru/2017/02/kak-vskryit-do-70-paroley-za-neskolko-minut/ (дата обращения: 20.09.2018).