Кресан Евгений Александрович
Главный эксперт отделения
компьютерных экспертиз
отдела фоноскоптческих и компьютерных экспертиз
экспертно-криминалистического центра
ГУ МВД России по Красноярскому краю

Kresan Evgeniy A.
Chief expert of the department of computer expertise
6 department (phonoscopic and computer expertise) Forensic Center
MIA General Administration for the
Krasnoyarsk Territory
E-mail: kresan@mail.ru

ШИФРОВАНИЕ ПАМЯТИ УСТРОЙСТВ, ИССЛЕДУЕМЫХ В РАМКАХ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ. КЛАССИФИКАЦИЯ. МЕТОДЫ ИССЛЕДОВАНИЯ

ENCRYPTION OF MEMORY OF DEVICES, EXAMINATED WITHIN COMPUTER EXPERTISE. CLASSIFICATION. METHODS OF RESEARCH

Аннотация: Статья посвящена современному состоянию и перспективным методам исследования шифрованной информации в памяти устройств под управлением различных операционных систем. В работе произведена классификация методов шифрования в зависимости от типа операционной системы. Приведены возможные пути решения задачи поиска ключевой информации и дешифрования пользовательских данных. Затрагиваются вопросы правового регулирования исследования информации на удаленных серверах («в облаке»).

Abstract: The article is devoted to the current state and perspective methods of studying encrypted information in device memory under the control of various operating systems. The classification of encryption methods is performed depending on the type of operating system. Possible ways of solving the problem of searching for key information and deciphering user data are presented. The issues of legal regulation of information research on remote servers ("in the cloud") are touched upon.

Ключевые слова: шифрование, Android, AES, BitLocker, Windows Account, iOS

Keywords: encryption, Android, AES, BitLocker, Windows Account, iOS.

Благодаря развитию экспертно-криминалистических средств и методов исследования информации, имеющейся в памяти мобильных устройств, сотрудники лабораторий компьютерных экспертиз массово используют технологии JTAG (и подобные) и chip-off. Анализ опыта, накопленного в ходе исследования устройств на базе различных операционных систем, позволяет

выделить проблему шифрования данных пользователя стандартными средствами операционных систем «на лету» как наиболее актуальную и не имеющую однозначного (универсального) технического решения. Пробел в законодательстве, которое регулировало бы получение ключевой информации из «облачных» ресурсов (удаленных серверов) в рамках проведения компьютерных экспертиз и исследований, также не позволяет использовать весь доступный эксперту инструментарий.

В рамках статьи предлагается классификация шифрования пользовательских данных стандартными средствами по типу операционной системы мобильного устройства.

Наиболее часто встречаются устройства на базе операционной системы Android различных версий. Впервые полнодисковое шифрование (full disk encryption – FDE) пытались внедрить еще в планшетной версии Android 3.0 Honeycomb. Тогда вместе с ядром Linux 2.6.36 в ней появился модуль dm-crypt, обеспечивающий возможность шифрования на любом блочном устройстве хранения данных (включая NAND Flash). В универсальной четвертой версии Android шифрование было доступно, однако для большинства оставалось невостребованной опцией. Из-за отсутствия программных оптимизаций и низкой скорости встраиваемых процессоров того времени включение шифрования приводило к падению производительности ввода-вывода в 6–8 раз на топовых моделях и до 20 раз – на бюджетных.

Исправить ситуацию удалось только с появлением 64-битных процессоров, имеющих отдельный набор инструкций для ускорения криптографических вычислений. Обязательным шифрование в Android стало только с версии 5.0, предустанавливаемой на устройства с современными однокристальными системами.

При этом есть принципиальная разница между тем, было ли устройство обновлено до Android 5.x или новее либо сразу выпускалось с такой версией. Во втором случае шифрование данных будет выполняться всегда. В первом варианте (при обновлении) оно останется опциональным и может быть отключено сбросом до заводских настроек.

В общем случае для полнодискового шифрования в Android используются три битовые последовательности: мастер-ключ, соль и пользовательский пин-код. Мастер-ключ и соль генерируются автоматически, а пин-код вводится владельцем устройства. Роль пин-кода может также выполнять пароль, графический ключ или любой другой «секрет» – для процессора это все равно битовая последовательность, причем довольно короткая.

В Android 7.0 появилась принципиально новая функция – пофайловое шифрование (file based encryption – FBE), которое выполняется с использованием возможностей файловой системы ext4. Новая реализация шифрования требует наличия аппаратно изолированной среды (trusted execution environment) с поддержкой API Keymaster 1.0 (старые версии 0.xx не подходят). Выполнение алгоритма AES процессором должно обеспечивать расшифровку данных со скоростью не менее 50 Мбайт/с.

До появления Android 7.0 при активации FDE все данные хранились

зашифрованными общим паролем, поэтому смартфоном невозможно было пользоваться до ввода пароля. Теперь же отдельные приложения (например, будильник) можно сделать доступными прямо на экране блокировки.

На устройстве с активным пофайловым шифрованием у пользователя появляется две области хранения данных приложений: зашифрованная отдельным паролем (Credential Encrypted – CE) и зашифрованная общим ключом устройства (Device Encrypted – DE). При отключении FBE обе области (CE и DE) остаются открытыми для любого приложения. При активном шифровании файлы области CE расшифровываются только после ввода пользовательского пароля. Файлы DE могут быть расшифрованы сразу после загрузки [1].

Следующим пунктом классификации выступают устройства, функционирующие под управлением операционной системы Windows. В частности, стоит обратить внимание на связку системы аутентификации Windows Account и встроенной системы шифрования BitLocker.

Для многих классов устройств использование Microsoft Account для входа в систему автоматически включит шифрование данных. Если устройство под управлением Windows 8, 8.1, 10 или Windows RT (планшет, ультрабук или устройство 2-в-1) поддерживает режим Connected Standby, укомплектовано модулем TPM2.0, если оперативная память фиксирована и в качестве системного накопителя используется флеш-память (eMMC, UFS2.0 или SSD), устройство готово к использованию системы защиты данных BitLocker Device Protection.

Для того чтобы шифрование активировалось, пользователю достаточно в процессе установки Windows ввести учетные данные Microsoft Account или в любой момент после добавить данные Microsoft Account к любой учетной записи с административными привилегиями – и Windows автоматически начнет шифрование системного раздела. Пользователь может ничего не знать о шифровании, но оно будет активировано – точно так же, как в смартфонах с заводской прошивкой на основе Android 6.0 и более новых.

Для входа в систему и расшифровки данных теперь достаточно ввести пароль от учетной записи Microsoft Account или воспользоваться упрощенной системой аутентификации Windows Hello (вход с помощью короткого пин-кода или биометрической аутентификации). При этом число попыток подбора пин-кода ограничено, а пароля к учетной записи Windows – нет. Более того, при попытке извлечь жесткий диск и подключить его к другому компьютеру потребуется ввести ключ шифрования BitLocker – просто данных учетной записи Microsoft Account уже недостаточно.

Казалось бы, такая система повышает безопасность информации, однако ключ шифрования, который применяется BitLocker Device Protection для доступа к системному разделу, хранится в Microsoft OneDrive и может использоваться тем, у кого есть доступ к учетной записи Microsoft Account пользователя.

Этого ключа будет достаточно для полной расшифровки зашифрованного тома как на компьютере пользователя (с загрузкой в Windows PE), так и при

переносе диска на другой компьютер.

Если диск зашифрован с помощью BitLocker или его «облегченной» версии – BitLocker Device Protection и при этом в системе установлен модуль TPM 2.0, извлечь базу данных SAM (в целях попытки подбора пароля для входа в Windows) будет невозможно или очень трудно. Существуют сложные атаки с помощью методов, для которых требуется физическое извлечение модулей оперативной памяти для попытки считать ключ шифрования (именно поэтому одно из требований для автоматической активации BitLocker Device Protection – несъемные (распаянные) модули оперативной памяти). Однако на логическом уровне такая защита достаточно безопасна.

Наличие Microsoft Account здесь – самое слабое звено. Если системный диск зашифрован и в компьютере активирован модуль TPM 2.0, извлечь SAM (например, с помощью Elcomsoft System Recovery) не получится.

В отличие от данных локальных учетных записей Windows, учетные записи Microsoft хранятся удаленно, в «облачном» сервисе Microsoft. Прямой перебор паролей (атакой на серверы Microsoft) невозможен. В то же время на локальном компьютере параметры учетной записи тоже хранятся. Это делается, чтобы пользователь мог зайти в Windows, даже если сетевое соединение недоступно. Данные о таких учетных записях можно попытаться извлечь, после чего попробовать восстановить пароль.

Пароль к онлайновой учетной записи Microsoft Account восстанавливается с помощью офлайновой атаки [2].

Наиболее стойкими к получению физического доступа к содержимому внутренней памяти на протяжении продолжительного времени являются устройства под управлением операционных систем семейства iOS.

В каждом устройстве с iOS имеется специализированный криптографический модуль AES-256, который встроен непосредственно в канал DMA между флеш-памятью и основной системной памятью для повышения эффективности шифрования файлов. На устройствах с процессором A9 или более новым (серии A) подсистема флеш-памяти находится на изолированной шине, которая получает доступ к памяти с пользовательскими данными только через криптографический модуль DMA.

Уникальный идентификатор устройства (UID) и идентификатор группы устройств (GID) – это 256-битные ключи AES, вшитые (UID) или скомпилированные (GID) в процессор программ и Secure Enclave на этапе производства. Ни одна программа или микропрограмма не может прочитать их напрямую; им доступны только результаты операций шифрования и дешифрования, выполненных специализированными модулями AES микросхемы с использованием UID или GID в качестве ключа. Кроме того, UID и GID подсистемы Secure Enclave могут быть использованы только специализированным AES-модулем Secure Enclave. Идентификаторы UID и GID также недоступны через JTAG и другие интерфейсы отладки.

На процессорах T1, S2, S3 и A9, а также более новых (серии A) каждый сопроцессор Secure Enclave генерирует собственный UID (уникальный идентификатор). Поскольку UID уникален для каждого устройства и

генерируется полностью внутри Secure Enclave, а не в производственной системе за пределами устройства, компания Apple и любые ее поставщики не могут получать доступ к UID или сохранять его. Программное обеспечение, работающее в Secure Enclave, задействует UID для защиты данных на устройстве.

UID обеспечивает возможность криптографической привязки данных к конкретному устройству. Например, UID входит в иерархию ключей, используемых для защиты файловой системы, поэтому при физическом перемещении микросхем памяти из одного устройства в другое файлы будут недоступны. UID не связан с другими идентификаторами устройства.

GID является общим для всех процессоров в определенном классе устройств (например, для всех устройств с процессором Apple A8). За исключением UID и GID, остальные криптографические ключи создаются системным генератором случайных чисел с использованием алгоритма на основе CTR_DRBG. Источником энтропии системы являются колебания времени при загрузке, а также колебания времени обработки прерываний после загрузки устройства.

Для генерирования ключей внутри Secure Enclave используется аппаратный генератор истинно случайных чисел: в его основе лежат несколько кольцевых генераторов, сигнал которых обрабатывается генератором CTR_DRBG.

Надежное стирание сохраненных ключей так же важно, как их генерирование. Особую сложность представляет стирание содержимого флеш-памяти: например, из-за алгоритма нивелирования износа может потребоваться стереть несколько копий данных. Для решения этой проблемы в устройствах с iOS предусмотрена специальная функция, предназначенная для надежного стирания данных. Она называется «Стираемый накопитель». Эта функция обращается к базовой технологии накопителя (например, NAND), чтобы получить прямой доступ и очистить небольшое количество блоков на очень низком уровне.

Помимо функций аппаратного шифрования, встроенных в устройства iOS, Apple использует специальную технологию для более надежной защиты данных, хранящихся во флеш-памяти на устройстве.

Технология защиты данных позволяет устройству реагировать на обычные события, такие как поступление телефонного вызова, а также обеспечивает более высокий уровень шифрования данных пользователей. Основные системные программы, такие как «Сообщения», «Почта», «Календарь», «Контакты», «Фото» и «Медданные», используют технологию защиты данных по умолчанию, а программы сторонних разработчиков, установленные в iOS 7 или более поздней версии, получают ее автоматически.

Защита данных осуществляется путем построения и контроля иерархии ключей и основана на технологиях аппаратного шифрования, встроенных в каждое устройство iOS. Защита данных организована на уровне файлов: каждому из них назначается один из классов защиты, а доступность определяется разблокированием ключей класса. С появлением файловой системы Apple (APFS) файловая система стала способна к дальнейшему разделению ключей по интервалам (различные фрагменты файла могут иметь

разные ключи) [3].

Подводя итоги рассмотрения трех наиболее популярных операционных систем, имеющих в составе модули шифрования пользовательских данных, стоит отметить, что получение доступа к информации пользователя посредством атаки «в лоб», «перебором» нецелесообразно ввиду значительных временных и аппаратных затрат. В качестве положительного опыта получения ключевой информации, необходимой для расшифровки пользовательских данных, можно выделить проведение следственных действий – осмотров (с обязательной пошаговой фиксацией действий и результатов в протоколе) «облачных» сервисов, а также исследование в рамках одного следственного действия нескольких устройств, о которых достоверно известно, что они принадлежали одному лицу.

На базе 6 отдела ЭКЦ ГУ МВД России по Красноярскому краю ведется база данных мобильных устройств, которые ранее поступали на экспертизу, исследование либо осмотр, где фиксируется, как и с помощью каких программных или аппаратных средств был получен доступ к содержимому внутренней памяти конкретного устройства. Указывается, возможно ли получение доступа, если учетные данные (имя пользователя, пароль, пин-код, графический ключ и т.п.) неизвестны, установлено ли шифрование памяти «по умолчанию», заблокирован ли загрузчик операционной системы, имеется ли возможность установки модифицированной консоли восстановления (recovery TWRP, CWM и т.п.). Для систематизации и ускорения процесса исследования памяти мобильных устройств в ряде регионов ведутся подобные базы данных. В свете изложенного предлагается объединить усилия и создать единую базу данных, которая бы аккумулировала знания экспертов о той или иной модели мобильного устройства, но уже в масштабах страны.

Список литературы

1. Шифрование данных в Андроид. Как это работает. [Электронный ресурс] // Cryptoworld практическая безопасность. 2017. 4 марта. URL: http://cryptoworld.su/shifrovanie-dannyx-v-android-kak-eto-rabotaet (дата обращения: 25.09.2018).

2. Афонин О. Microsoft Account: удобство или дыра в безопасности? [Электронный ресурс] // Блог Элкомсофт 2017. 28 февраля. https://blog.elcomsoft.com/ru/2017/02/microsoft-account-udobstvo-ili-dyira-v-bezopasnosti (дата обращения: 25.09.2018).

3. Безопасность iOS. iOS 11. Январь 2018 г. Систем. требования: Adobe Acrobat Reader. URL: https://www.apple.com/ru/business/docs/iOS_Security_Guide.pdf (дата обращения: 25.09.2018).