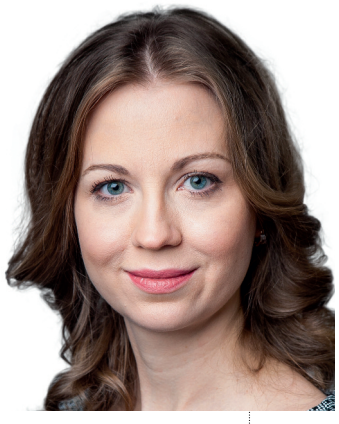
Криптография и клептография: скрытые каналы и лазейки в криптоалгоритмах

Алексей Жуков, *председатель совета Ассоциации "РусКрипто"*
Александра Маркелова, *технический директор ООО "НТЦ Альфа-Проект", к. ф.-м. н.*

В последнее время наблюдаются попытки государственных структур ряда ведущих стран ослабить алгоритмы шифрования и стандарты безопасности с целью облегчения работы спецслужб и правоохранительных органов в рамках мер, предпринимаемых государством в ответ на рост террористической опасности. В числе прочего следуют заявления об обязательном внедрении лазеек в криптоалгоритмы, являющиеся государственными стандартами. Не касаясь этических, юридических, экономических и политических сторон, рассмотрим этот процесс с криптографической точки зрения: какие модели и механизмы лежат в основе той или иной криптографической лазейки, можно ли ее обнаружить, кто может воспользоваться теми возможностями, которые она предоставляет.



"Война – это мир, рабство – это свобода, ослабление криптоалгоритмов – это безопасность киберпространства", – пожалуй, именно эта формулировка наиболее точно отражает содержание речи заместителя генерального прокурора США Рода Розенштейна[1]. Выступая в октябре 2017 г. перед выпускниками Военно-морской академии, он в который раз сформулировал официальную позицию властей и спецслужб США: надежное шифрование – антиконституционно[2], потому что мешает правоохранительным органам эффективно бороться с преступностью как на этапе предотвращения преступлений, так и при проведении расследований.

По мнению генерального прокурора, именно прозрачность (для наблюдения) киберпространства делает его безопасным для всех участников.

Речь генерального прокурора является частью процесса, еще несколько десятилетий тому назад названного западной прессой "криптовойнами". Этим термином характеризуется то скрытое, то явное стремление со стороны государства ограничить общественность в доступе к криптографическим средствам, обеспечивающим сильную защиту. Среди причин, как правило, указывают на недопустимость попадания надежных систем шифрования в руки террористов, организованной преступности или недружественных режимов.

Криптография и жизнь

На сегодняшний день подавляющее большинство людей так или иначе используют криптографию в повседневной жизни: в мобильной телефонной связи, в банковских картах, при использовании безопасной передачи информации по протоколам SSL/TLS в интернет-браузерах и т.п. Появляется все больше бытовых приборов (телевизоров, кофеварок, пылесосов), подключенных к так называемому Интернету вещей (IoT, Internet-of-Things), и конечно же, коммуникации этих устройств между собой и с владельцем должны быть надежно защищены криптографическими методами. Даже автомобили становятся частью Интернета вещей (развитие концепции Connected Car), и это уже вопрос безопасности не только ценной личной информации, но и жизни водителя.

Все это принято относить к "гражданской[3] криптографии" – т.е. криптографии, которая, в отличие от криптографии государственной или военной, призвана удовлетворять потребности частных лиц и организаций.

ГОСТ Р 51275–2006 [5]:

Программная закладка – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

[1] *Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryp-tion at the United States Naval Academy. Annapolis, MD ~ Tuesday, October 10, 2017. https://www.justice.gov/opa/speech/ deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.*

[2] *Дословно: "Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety" и "There is no constitutional right to sell warrant-proof encryption".*

[3] *Прилагательное "гражданская" юридического и политологического смысла здесь не несет.*

Криптография и преступность

Одновременно с этим среди пользователей гражданской криптографии оказываются не только законопослушные граждане, но и преступники, мошенники, террористы, использующие современные технологии для подготовки, совершения и сокрытия преступлений. Криптография в их руках с точки зрения правоохранительных органов – безусловно, очень неудобное и опасное оружие.

Одним из наиболее значимых явлений международной и внутриполитической жизни в начале XXI в. стал терроризм. В связи с ростом террористических угроз общество требует принятия мер, в том числе и самых жестких. Государство "с удовольствием" идет навстречу таким пожеланиям. Антитеррористические меры, предпринимаемые со стороны государства, касаются и вопросов криптографии.

Усиление вторжения государства в гражданскую криптографию – вполне ожидаемая и неизбежная реакция государственных институтов, и прежде всего законодателей и спецслужб. Все больше и больше официальных лиц заявляют о необходимости принятия на официальном государственном уровне решения о внедрении уязвимостей в информационные системы, сети и пользовательские устройства, об обязательном внедрении лазеек в криптоалгоритмы, являющиеся государственными стандартами. В настоящее время известно как минимум о двух алгоритмах, снабженных потайным ходом и утвержденных при этом в США в качестве федеральных стандартов – Skipjack (Clipper chip) [2] и Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) [3]. Последний был успешно продвинут в международные стандарты[4] [4].

Криптография и общество

Последнее время в СМИ все чаще появляются сообщения о лазейках и потайных ходах в криптоалгоритмах. Раньше этот аспект деятельности был, по всеобщему мнению, исключительной прерогативой "плохих парней", пытающихся похитить ваши секреты (в том числе и финансовые). В частности, с этих позиций был написан обзор [1]. Теперь же регулярно возникает вопрос о легитимизации подобных мер со стороны государства. Жизнь ставит вызовы, на которые приходится отвечать так или иначе. Уровень терроризма растет, и общество требует принятия ответных мер. Не впадая в пафос слов о свободах и правах человека, следует осознать, что перед всеми (и в том числе перед нами) стоит трудный выбор – гарантированное ограничение свобод или возможная угроза десяткам, сотням, а то и тысячам жизней. Однозначного решения – увы! – не существует. Выбор очень непростой, и любое решение вызовет неоднозначные оценки.

"Война – это мир, рабство – это свобода, ослабление криптоалгоритмов – это безопасность киберпространства", – пожалуй, именно эта формулировка наиболее точно отражает содержание речи заместителя генерального прокурора США Рода Розенштейна1. Выступая в октябре 2017 г. перед выпускниками Военно-морской академии, он в который раз сформулировал официальную позицию властей и спецслужб США: надежное шифрование – антиконституционно2, потому что мешает правоохранительным органам эффективно бороться с преступностью как на этапе предотвращения преступлений, так и при проведении расследований.

Даже среди экспертов в области криптографии мнения разделились, хотя в своем большинстве криптографическое сообщество настроено против подобных мер. Объясняется это не только либеральными настроениями, традиционно главенствующими в умах (западной) интеллигенции, это неприятие имеет под собой и более серьезную базу.

Возросшая активность спецслужб и прочих ведомств по ослаблению действующих криптоалгоритмов невероятно опасна. Опасна не только мало контролируемой возможностью доступа к корреспонденции всех граждан, а не только террористов, но и тем, что нет никаких гарантий того, куда и кому пойдет эта информация. Ключи к потайному ходу криптоалгоритма значительно проще похитить и использовать, чем другие типы оружия массового поражения (базы ГИБДД и МГТС, свободно продававшиеся на Горбушке, тому пример). Лазейки, призванные защитить нас от терроризма, могут сами стать оружием террористов в случае утечки ключа, например, если это лазейка в Connected Car, позволяющая получить удаленное управление автомобилем.

В любом случае тотальный запрет на использование гражданского шифрования малореалистичен в силу целого ряда экономических причин, а также практической невозможности полного контроля над трафиком и приложениями, установленными на устройствах пользователей. Нельзя также забывать и про неотъемлемое право честных пользователей на защиту своих данных.

Криптография и будущее

Все это, судя по всему, может стать (обще)мировой тенденцией с которой нельзя будет не считаться. Мы живем не в изолированном мире, и эти тенденции неизбежно коснутся и нас.

Современная криптография – область на стыке математики, математической кибернетики и прикладных инженерно-технических наук. И никакой раздел математики или кибернетики не является столь связанным с повседневной жизнью, столь политизированным и, вследствие этого, столь подверженным воздействию со стороны государства, как криптография. Вероятно, поэтому в криптографические споры зачастую втя-

Слабые закладки – это намеренное ослабление алгоритма, позволяющее узнать секретную пользовательскую информацию на основе открытой информации.

Скрытый канал (Covert Channel): непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Усиление вторжения государства в гражданскую криптографию – вполне ожидаемая и неизбежная реакция государственных институтов, и прежде всего законодателей и спецслужб. Все больше и больше официальных лиц заявляют о необходимости принятия на официальном государственном уровне решения о внедрении уязвимостей в информационные системы, сети и пользовательские устройства, об обязательном внедрении лазеек в криптоалгоритмы, являющиеся государственными стандартами.

[4] Более подробно об этом будет рассказано в следующих работах.

гиваются люди, совершенно далекие от математики (например, вопрос о том, возможно ли – и как – читать сообщения защищенных чатов мессенджера Telegram, не обсуждал только ленивый). Эти люди зачастую предлагают не самые адекватные (с точки зрения криптографии) решения. Так, например, уже упомянутый в начале статьи Род Розенштейн считает, что вопросы доступа спецслужб к зашифрованной информации можно решить по аналогии с системой распространения лицензионных ключей и ключей обновления программного обеспечения. И тут снова можно вспомнить и про Горбушку, и про торрент-трекеры[5].

А существуют ли надежные методы обеспечения эксклюзивного доступа спецслужб к пользовательской информации при сохранении достаточного уровня стойкости от стороннего нарушителя? Авторы планируют посвятить этому вопросу цикл статей. В них будут рассмотрены различные аспекты клептографии[6] – деятельности по внедрению уязвимостей в математическую структуру криптографических систем и пользовательских устройств.

Не касаясь этических, юридических, экономических и политических сторон этого явления, рассмотрим его с криптографической, а точнее – с математической точки зрения: какие математические модели и механизмы лежат в основе механизма той или иной клептографической лазейки, можно ли обнаружить лазейку, кто может воспользоваться теми возможностями, которые она предоставляет, и какие меры противодействия существуют, – со всем этим мы и постараемся разобраться в статьях, которые планируется опубликовать в ближайших выпусках журнала.

Проблема существования лазеек в криптографических системах

Окружающая нас информационная среда включает разнообразные программно-аппаратные средства для решения задач информационной безопасности, в том числе программно и аппаратно реализованные криптографические алгоритмы, которые для пользователей зачастую представляются как черные ящики. Это или аппаратные устройства шифрования, логика которых реализована на низком уровне, или пакеты программ, часто без наличия исходных текстов. Конкретную структуру алгоритма сложно отследить даже в программных продуктах при отсутствии текстов исходных программ. И даже в тех случаях, когда спецификация становится доступной для пользователя, последний весьма редко проверяет соответствие имеющегося в его распоряжении продукта официальной документации. Таким образом, пользователи зачастую получают лишь иллюзию защиты. Используя алгоритм, все детали работы которого известны только его разработчику, пользователь располагает единственной гарантией стойкости – утверждением самого разработчика о надежности алгоритма. В то же время разработчики готовых продуктов объективно имеют возможность встроить лазейки в реализуемые криптографические алгоритмы по своей ли инициативе, по чьему-либо заказу или по указанию "сверху".

Другой способ подтверждения безопасности кода – сертификация (например, на соответствие Common Criteria или на соответствие отраслевым стандартам, таким как EMV для банковских карт) – к сожалению, тоже не всегда безупречен. Причина в том, что зачастую, хотя международные сертификационные лаборатории и являются формально независимыми, но реально их деятельность все равно подчиняется локальному законодательству в области информационной безопасности, т.е. спецслужбе той страны, где лаборатория расположена.

Таким образом, сертификация может защитить от недобросовестного разработчика, но не гарантирует отсутствия правительственных закладок.

В итоге вопрос состоит в том, что может сказать пользователь о той конкретной реализации криптографического алгоритма, которая находится в его распоряжении. Насколько в действительности она его защищает? Насколько легко производителям программных продуктов и аппаратных модулей безопасности встроить лазейку в свою продукцию так, что она останется незамеченной, но в то же время позволит производителю нарушить конфиденциальность пользователя?

Итак, основными вопросами, возникающими при пользовании криптографическими черными ящиками, являются:

1. Предоставляет ли данная реализация алгоритма недокументированные возможности и, в частности, содержит ли она незаявленные включения, позволяющие реализовать недокументированные возможности?
2. Имеет ли место утечка секретной информации?
3. Возникает ли риск для пользователя в случае успешного реверсинжиниринга данного продукта третьей стороной?

Встроенные каналы утечки информации (лазейки)

Облегченный доступ ко всем данным, имеющимся в информационном пространстве, может быть обеспечен либо за счет явного ослабления механизмов защиты информационных систем и пользовательских устройств, либо путем введения в структуру алгоритмов замаскированных лазеек. По своей сути лазейки являются встроенными каналами утечки информации. Модифицированные таким образом криптосистемы называют также зараженными (или инфицированными) криптосистемами.

К сожалению, сложившейся, общепризнанной терминологии в этой области пока нет. Даже в англоязычной литературе, насчитывающей несколько сотен работ, написанных за несколько последних десятилетий и посвященных закладкам-лазейкам, нет устоявшегося мнения относительно того, как следует называть криптографические лазейки. Тем не

При анализе работы клептографических систем традиционно выделяют следующих трех участников [1]:

- разработчик – обладает информацией о лазейке, владеет секретным ключом к лазейке, не владеет секретным ключом пользователя;
- пользователь – владеет секретным ключом пользователя, в случае успешного реверс-инжиниринга обладает информацией о лазейке, но не владеет ее секретным ключом;
- злоумышленник – в случае успешного реверс-инжиниринга обладает информацией о лазейке, но не владеет ее секретным ключом, а также секретным ключом пользователя.

Пользователи зачастую получают лишь иллюзию защиты. Используя алгоритм, все детали работы которого известны только его разработчику, пользователь располагает единственной гарантией стойкости – утверждением самого разработчика о надежности алгоритма. В то же время разработчики готовых продуктов объективно имеют возможность встроить лазейки в реализуемые криптографические алгоритмы по своей ли инициативе, по чьему-либо заказу или по указанию "сверху".

[5] Напоминаем, что многие торрент-трекеры в РФ заблокированы Роскомнадзором за нарушение авторских прав, но технические способы обхода блокировок существуют (авторы статьи не одобряют подобные методы, т.к. это нарушает российское законодательство).

[6] Термин появился благодаря работам А. Янга и М. Юнга (Adam Young, Moti Yung).

менее большинство авторов (и авторы данной статьи разделяют это мнение) предлагают закрепить за криптографическими лазейками термин Backdoors, оставив термин Trapdoors для обозначения информации, позволяющей легко обратить однонаправленную функцию (Trapdoor one-Way Function).

Программная закладка

В русскоязычной литературе для обозначения этих понятий используются и "закладки", и "лазейки", и "бэкдоры", и даже "потайные ходы". Термин "закладка" зафиксирован в ГОСТ Р 51275–2006 [5]: программная закладка – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

В данной статье авторы будут использовать и "лазейки", и "закладки", и "бэкдоры" как синонимы.

Для построения или обнаружения лазеек необходимо ответить на следующие вопросы.

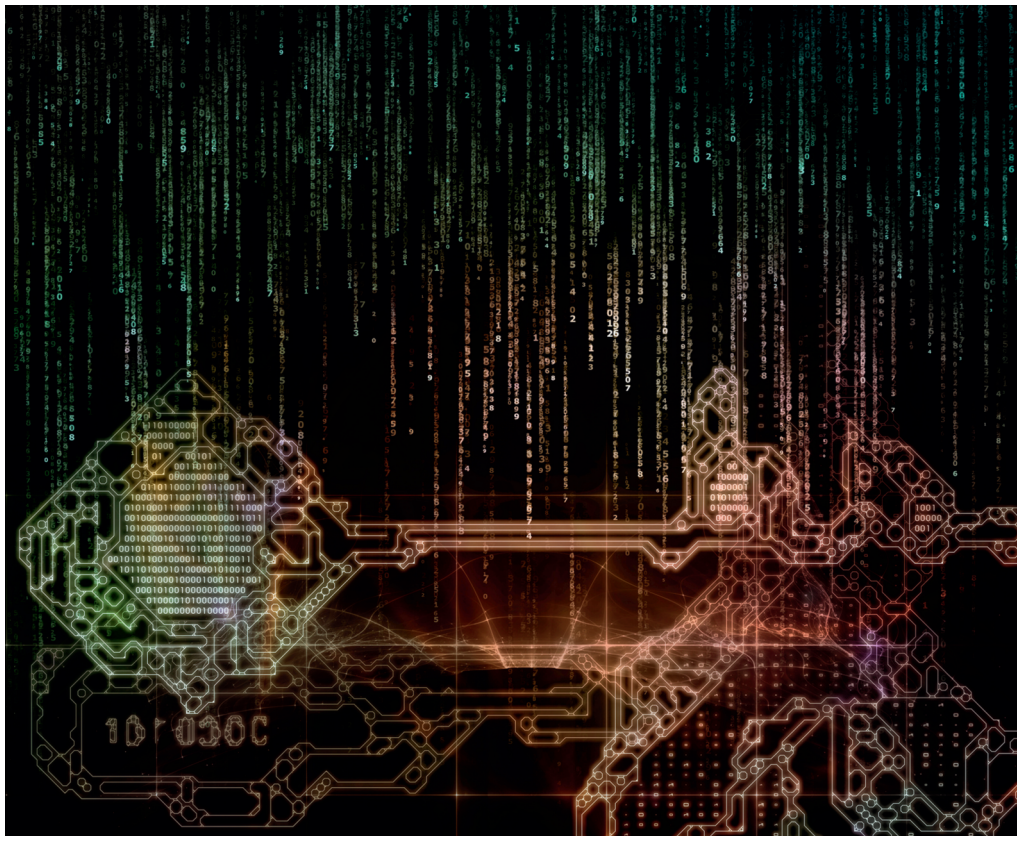
1. Какая информация выдается с устройства?
2. Может ли устройство содержать скрытый канал утечки информации?
3. Если может, то какова пропускная способность этого канала?
4. Что можно скрыть в выдаваемой информации, не мешая при этом нормальной работе устройства?
5. Какие дополнительные данные необходимо знать, чтоб извлечь из выдаваемой информации скрытые в ней данные? (То есть что является ключом к лазейке?)

Слабые закладки

Способы встраивания закладок в криптографические алгоритмы можно условно разделить три основных группы: слабые закладки, передача информации по скрытым каналам, SETUP-механизмы [6].

Слабые закладки – это намеренное ослабление алгоритма, позволяющее узнать секретную пользовательскую информацию на основе открытой информации.

Слабые закладки всегда обнаруживаются с помощью реверсинжиниринга. В ряде случаев слабые закладки можно выявить, основываясь только на выходных (открытых) данных алгоритма, с помощью простых алгебраических проверок или статистического анализа. Подробнее о теоретических способах построения слабых закладок можно прочитать в [11], а о некоторых реальных случаях обнаружения подобных уязвимостей (на примере алгоритма RSA) – в [10].



Современная криптография – область на стыке математики, математической кибернетики и прикладных инженерно-технических наук. И никакой раздел математики или кибернетики не является столь связанным с повседневной жизнью, столь политизированным и, вследствие этого, столь подверженным воздействию со стороны государства, как криптография.

Скрытые каналы

Вопрос о существовании лазеек в криптографическом алгоритме тесно связан с понятием скрытого канала передачи информации.

В соответствии с ГОСТ Р 53113.1–2008 [9] скрытый канал (Covert Channel) – непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

То есть канал называется скрытым, если он специально не проектировался и изначально не предполагался для передачи информации в электронной системе обработки данных. На практике к таким каналам относят не только нестандартные каналы передачи информации, но и нестандартные способы передачи информации по легальным каналам. Примером такого канала является передача информации с помощью младших битов пикселей в файле с изображением.

Выбранная терминология представляется не совсем удачной. Как отмечено в [1], называть эти каналы скрытыми, тайными (hidden, covert) можно только при условии, что об их существовании ничего не известно. В противном случае третье лицо, имеющее информацию об этих каналах, в ряде случаев будет получать всю информацию, проходящую по ним, и даже иметь возможность изменять эту информацию по своему усмотрению. Поэтому, на наш взгляд, такие каналы уместнее называть нестандартными или нелегальными.

Для построения или обнаружения лазеек необходимо ответить на следующие вопросы.

1. Какая информация выдается с устройства?
2. Может ли устройство содержать скрытый канал утечки информации?
3. Если может, то какова пропускная способность этого канала?
4. Что можно скрыть в выдаваемой информации, не мешая при этом нормальной работе устройства?
5. Какие дополнительные данные необходимо знать, чтоб извлечь из выдаваемой информации скрытые в ней данные?

основными вопросами, возникающими при пользовании криптографическими черными ящиками, являются:
1. Предоставляет ли данная реализация алгоритма недокументированные возможности и, в частности, содержит ли она незаявленные включения, позволяющие реализовать недокументированные возможности?
2. Имеет ли место утечка секретной информации?
3. Возникает ли риск для пользователя в случае успешного реверсинжиниринга данного продукта третьей стороной?

Мы также будем рассматривать другой вид скрытых каналов, называемых в английской терминологии Subliminal[7]. К этому виду относятся скрытые каналы передачи информации, воспользоваться которыми может только обладатель соответствующей информации (ключа к скрытому каналу) [1]. Будем называть такие каналы защищенными скрытыми каналами.

Пропускная способность скрытого канала – это количество информации, которое может быть передано по скрытому каналу в единицу времени или относительно какой-либо другой шкалы измерения [9]. Это определение корректно для обоих видов скрытых каналов (Covert и Subliminal). Мы будем оценивать пропускную способность скрытого канала относительно количества информации, передаваемой по основному каналу.

Пропускная способность скрытого канала – это количество информации, которое может быть передано по скрытому каналу в единицу времени или относительно какой-либо другой шкалы измерения [9]. Это определение корректно для обоих видов скрытых каналов (Covert и Subliminal).

Например, если пропускная способность равна 1/2, то это означает, что на n бит, переданных по основному каналу, мы можем передать n/2 бит информации по скрытому каналу.

Криптоалгоритмы с лазейками. SETUP-механизмы

Криптоалгоритм с лазейкой (Backdoor, Trapdoor) – это алгоритм, который содержит некоторую скрытую структуру (лазейку), обеспечивающую существование скрытого канала передачи информации; знание этой структуры позволяет получать секретную информацию (например, о секретном ключе). Без знания лазейки алгоритм кажется надежным.

Наибольший интерес среди них представляют клептографические лазейки, названные в [7], [8] SETUP-механизмами (SETUP – Secretly Embedded Trapdoor with Universal Protection – секретно встроенная лазейка с универсальной защитой) – специальные видоизменения, внесенные в "добропорядочный" криптографический алгоритм с целью позволить разработчику лазейки получать секретную информацию (чаще всего о секретном ключе пользователя), но так, что внешне работа "инфицированного" алгоритма не отличается от работы "неинфицированного". Они отличаются от других видов закладок (программных, аппаратных, алгоритмических и т.п.) тем, что при их встраивании модифицируется математическая структура инфицируемого алгоритма. В отличие от классических недекларированных возможностей ПО, клептографические закладки, как правило, не изменяют алгоритмы работы системы в целом (т.е. не предоставляют нарушителю административные права доступа, не стирают пользовательские данные, не проводят записи в файлы, не отправляют e-mail и т.п.).

Более того, инфицированные клептографическим бэкдором протоколы могут даже не быть недокументированной возможностью ПО; в дальнейшем мы увидим, что некоторые алгоритмы с лазейками были частью международных стандартов, т.е. были документированы и использовались вполне легально.

При анализе работы клептографических систем традиционно выделяют следующих трех участников [1]:

- разработчик – обладает информацией о лазейке, владеет секретным ключом к лазейке, не владеет секретным ключом пользователя;
- пользователь – владеет секретным ключом пользователя, в случае успешного реверс-инжиниринга обладает информацией о лазейке, но не владеет ее секретным ключом;
- злоумышленник – в случае успешного реверс-инжиниринга обладает информацией о лазейке, но не владеет ее секретным ключом, а также секретным ключом пользователя.

Предполагается, что злоумышленник успешно применил реверс-инжиниринг к одному или нескольким устройствам (но не к данному) и получил код и содержимое их энергонезависимой памяти. Предполагается также, что злоумышленник имеет доступ ко всей публичной информации, включая общедоступные алгоритмы, открытые ключи, зашифрованные тексты, подписи и т.д. При этом в [11] выделяется два типа злоумышленника.

Отличительный злоумышленник. Его цель в том, чтобы отличить честную реализацию от нечестной.

Злоумышленник-криптоаналитик. Его цель состоит в том, чтобы сломать безопасность данного устройства, которое никогда не подвергалось реверс-инжинирии. Это может включать нахождение закрытого пользовательского ключа, дешифрование шифрования с открытым ключом, подделку подписи и т.д.

Принимая во внимание тенденции последних лет, ролевую модель можно видоизменить, добавив нового участника – спецслужбу и ограничив уровень знания разработчика [10]. В этой новой модели вместе с "пользователем" и "злоумышленником" действуют:

- спецслужба – обладает информацией о лазейке, владеет секретным ключом к лазейке, не владеет секретным ключом пользователя;
- разработчик – обладает информацией о лазейке, владеет открытым ключом лазейки, не владеет секретным ключом к лазейке, не владеет секретным ключом пользователя.

Спецслужба выдает разработчику инструкции по реализации лазейки и открытый ключ, с помощью которого будут шифроваться выдаваемые через лазейку пользовательские данные. Разработчик знает весь механизм работы, но не знает секретного ключа, поэтому при использовании не сможет полу-

[7] *Subliminal – подсознательный (англ.) – термин из психоанализа. Неудачность использования в данном контексте такого термина с точки зрения русского языка – очевидна.*

чить доступ к пользовательским данным (т.е. пользователь защищен не только от стороннего нарушителя, но и от разработчика). Злоумышленник до проведения реверс-инжиниринга обладает меньшими возможностями, чем разработчик.

SETUP-механизмы могут быть симметричными и асимметричными. По аналогии с симметричным шифрованием в симметричных лазейках ключ, встроенный в реализацию, совпадает с ключом автора лазейки, необходимым для получения доступа к скрытому каналу (или же эти ключи легко вычислимы друг из друга). С другой стороны, ключ разработчика асимметричной лазейки не может быть эффективно вычислен по данным, встроенным в реализацию инфицированного алгоритма. После обнаружения в реализации алгоритма асимметричного SETUP-механизма и выяснения его особенностей, например, при помощи реверс-инжиниринга и пользователи, и злоумышленники (все, за исключением владельца ключа к асимметричной лазейке) не могут определить как уже использованные, так и будущие секретные ключи пользователя. В этом смысле асимметричный SETUP-механизм обеспечивает "криптостойкость" системы по отношению ко всем нарушителям, кроме спецслужбы (в том числе и по отношению к разработчику) и может использоваться даже в системах с открытым исходным кодом.

Рассмотрим различные виды закладок на простом примере.

Читателю наверняка знаком алгоритм подписи RSA[8]. Как известно, перед формированием подписи данные обычно хэшируются. А поскольку размер хэша зачастую меньше размера открытого модуля RSA, то результат хэширования дополняется некоторыми фиксированными или случайными байтами.

Так, например, в стандарте PKCS#1 [12] описан метод выравнивания RSASSA-PSS, при котором в качестве выравнивающих данных используется некоторая случайная строка и некоторые преобразования этой строки. При проверке подписи данное значение легко восстанавливается, т.е. оно не является секретом и доступно любому наблюдателю, включая злоумышленника.

Нетрудно заметить, что salt можно использовать в качестве скрытого канала передачи данных, поскольку никаких ограничений на это значение нет и никаких дополнительных проверок оно проходить не должно.

Если передаваемая информация передается через salt в открытом виде, то это можно рассматривать как аналог слабой закладки. То есть любой сторонний нарушитель получает тот же доступ к информации скрытого канала, что и разработчик лазейки.

Если вместо salt передавать значение (salt)' = E(m'), где m'– передаваемая секретно информация, а E– функция шифрования, то получается лазейка с защитой (с ключом).

Если при этом E – симметричное шифрование, то это симметричная лазейка. В таком случае лазейка защищена только от стороннего нарушителя, не имеющего возможности провести реверс-инжиниринг.

Если же E – асимметричное шифрование, то мы построили асимметричную закладку, защищенную и от стороннего наблюдателя, и от злоумышленника, который провел реверс-инжиниринг, и от разработчика (в случае, если ключ расшифрования известен только спецслужбе).

Отметим также, что если функция E обеспечивает достаточно хорошую статистику на выходе, то случайное значение salt и вычисленное значение (salt)' полиномиально неразличимы, т.е. закладка устойчива даже против отличительного злоумышленника.

Данный пример, конечно же, является очень упрощенным и предназначен главным образом для иллюстрации темы. А более интересные и изощренные закладки мы обсудим в последующих работах.

Литература

[1] Жуков А.Е. Криптосистемы со встроенными лазейками // BYTE Россия. – 2007. – № 101. – С. 45–51.

[2] National Institute of Standards and Technology. Escrowed Encryption Standard.– NIST FIPS PUB 185, U.S. Department of Commerce, 1994.

[3] National Institute of Standards and Technology. Recommendation for Random Number Generation Using Deterministic Random Bit Generators.– NIST Special Publication 800-90A, Rev. 1, 2012. First version June 2006, second version March 2007, http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

[4] ISO/IEC 18031:2005. Information technology – Security techniques – Random bit generation.

[5] ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

[6] Маркелова А.В. Уязвимость ROCA и другие возможности внедрения закладок в алгоритм RSA. Всероссийская студенческая конференция "Студенческая научная весна": сборник тезисов докладов. – МГТУ им. Н.Э. Баумана, 2018. – С. 313–314.

[7] Young A., Yung M. Kleptography: using Cryptography against Cryptography // In book: EUROCRYPT'97. (Series: Lecture Notes in Computer Science). Springer, 1998. – Vol.1233. – Pp. 62–74.

[8] Young A., Yung M. Monkey – Black-Box Symmetric Ciphers Designed for MONopolizing KEYs // In book: FSE'98. (Series: Lecture Notes in Computer Science). Springer, 1998. – Vol.1372. – Pp. 122–133.

[9] ГОСТ Р 53113.1–2008. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

[10] Маркелова А.В. Скрытые каналы и лазейки с универсальной защитой в асимметричных криптоалгоритмах // Отчет по научно-исследовательской работе. – МГТУ им. Н.Э. Баумана, 2018. – 50 с.

[11] Young A., Yung M. Malicious Cryptography. Exposing Cryptovirology. Wiley Publishing, Inc. 2004.

[12] PKCS #1 v2.1: RSA Cryptography Standard. RSA Laboratories. DRAFT 1 – September 17, 1999.

SETUP-механизмы могут быть симметричными и асимметричными. По аналогии с симметричным шифрованием в симметричных лазейках ключ, встроенный в реализацию, совпадает с ключом автора лазейки, необходимым для получения доступа к скрытому каналу (или же эти ключи легко вычислимы друг из друга). С другой стороны, ключ разработчика асимметричной лазейки не может быть эффективно вычислен по данным, встроенным в реализацию инфицированного алгоритма. После обнаружения в реализации алгоритма асимметричного SETUP-механизма и выяснения его особенностей, например, при помощи реверс-инжиниринга и пользователи, и злоумышленники (все, за исключением владельца ключа к асимметричной лазейке) не могут определить как уже использованные, так и будущие секретные ключи пользователя. В этом смысле асимметричный SETUP-механизм обеспечивает "криптостойкость" системы по отношению ко всем нарушителям, кроме спецслужбы (в том числе и по отношению к разработчику) и может использоваться даже в системах с открытым исходным кодом.

[8] *Необходимую информацию можно найти практически в любой книге, посвященной криптографии, а также на нескольких сотнях сайтов с криптографической тематикой*