А. А. Шептунов, А. О. Пасько, А. С. Проничкин

АТАКИ НА МОБИЛЬНЫЕ УСТРОЙСТВА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ WI-FI

Введение

Мобильные телефоны занимают все более важное место в жизни любого современного человека, реализуя, помимо своих основных функций, огромное количество дополнительных возможностей: просмотр и редактирование документов, запись аудио и видео, навигацию с помощью спутника, доступ в Интернет, встроенный фотоаппарат и многое другое.

В настоящее время в мобильных устройствах для доступа к сети Интернет все чаще используется технология Wi-Fi беспроводной передачи данных. Во многом эта функция телефона компенсирует то, что на данный момент сотовые сети не имеют возможности передавать интернет-трафик с приемлемой скоростью. Кроме того, Интернет от сотового оператора пока достаточно дорог. Пользователи все чаще выходят в Интернет через бесплатные Wi-Fi точки доступа, которые, как правило, располагаются в кафе или торговых центрах.

В связи с таким широким распространением данной технологии нельзя не отметить, что на системы, реализованные с ее использованием, могут осуществляться атаки.

Рассмотрим принципы реализации Wi-Fi (стандарт IEEE 802.11) [1].

Режимы работы Wi-Fi сетей

В 802.11 сетях есть два режима работы: Ad-hoc и инфраструктура (управляемый через точки доступа).

Режим Ad-hoc используется, главным образом, для временных сетей, в которых компьютеры общаются друг с другом напрямую. В режиме инфраструктуры узлы связываются и обмениваются информацией через единственную точку доступа. Сеть может иметь много точек доступа, а клиенты — передвигаться между ними, переключаясь с одной на другую.

В сетях на основе точек доступа необходимо рассмотреть понятия идентификации и ассоциации. Прежде чем клиент может начать общаться с точкой доступа, ему необходимо подтвердить свою подлинность и только после этого послать запрос ассоциации.

Многие пользователи мобильных телефонов при настройке соединений просто оставляют 802.11 сети открытыми, так как не задумываются о том, что Wi-Fi сеть может быть уязвима.

Режимы идентификации устройств в Wi-Fi сетях

Существует два режима идентификации: открытая система и общедоступная идентификация (Shared Key).

Открытая система — это опознавательный алгоритм, в рамках которого любой может связаться с точкой доступа.

Общедоступная идентификация базируется на использовании протокола шифрования WEP (Wired Equivalent Privacy), который требует предварительного ввода секретного ключа. После успешного опознавательного запроса и ответа клиент может начать посылать данные.

Более того, точки доступа могут дополнительно зашифровать фреймы данных, используя алгоритм WEP.

Протокол WEP использует довольно нестойкий алгоритм шифрования RC4 на статическом ключе. Существует 64-, 128-, 256- и 512-битное WEP-шифрование. Чем больше бит используется для хранения ключа, тем больше существует возможных комбинаций ключей, а соответственно система обладает более высокой стойкостью к взлому. Часть WEP-ключа является статической

(40 бит в случае 64-битного шифрования), а другая (24 бит) — динамической (вектор инициализации), т. е. меняющейся в процессе работы сети.

Рассмотрим подробнее, как строится протокол WEP, обратив внимание на наиболее уязвимые стороны реализации данного метода защиты.

Общий вид работы протокола WEP представлен на рис. 1.

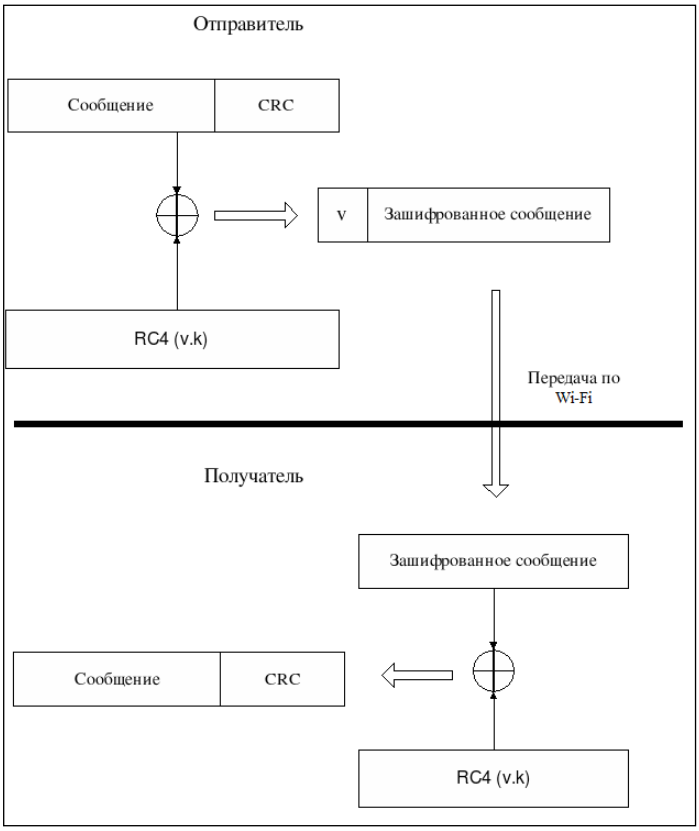

Рис. 1. Алгоритм работы протокола WEP

Итак, при передаче пакетов по Wi-Fi с использованием протокола WEP отправитель и получатель используют общий секретный ключ **k**, переданный по защищенному каналу.

Для того чтобы послать сообщение **M**, отправитель выполняет следующие действия.

Во-первых, он рассчитывает контрольную сумму сообщения **M** и прибавляет ее к самому сообщению. В итоге получается сообщение **P**.

Во-вторых, он выбирает вектор инициализации **v** и генерирует ключевой поток — последовательность случайных байт, зависящих от **v** и ключа **k**. Генерация происходит с использованием алгоритма шифрования **RC4**. На третьем шаге применяется операция **XOR** к **P** и ключевому потоку. В результате получается зашифрованное сообщение **C**.

C = P xor RC4(v,k)

Данный вектор передается по беспроводному каналу.

Получатель выполняет следующие действия:

Используя полученный вектор **v** и секретный ключ **k**, он генерирует ключевой поток на основе алгоритма шифрования **RC4.** Затем применяет операцию **XOR** к паре зашифрованного сообщения **C** и ключевого потока **RC4(v,k)**, получая сообщение **M',** для которого вычисляется контрольная сумма **c'**.

На третьем этапе проверяется равенство полученной и отправленной контрольных сумм. Если они равны, то исходное сообщение успешно передано.

WEP использует поточный шифр RC4 для генерации ключевого потока. Вся надежность протокола основана на защищенности этого алгоритма.

Один из главных параметров протокола WEP — это длина вырабатываемого ключа. Первоначальная реализация имела длину ключа в 64 бита: 40 бит непосредственно на ключ, используемый абонентами, и 24 бита на вектор инициализации. Существует версия протокола WEP с длиной ключа 128 бит. В таком случае сам ключ имеет длину 104 бита, а вектор инициализации — 24 бита.

Таким образом, предполагается, что достаточный объем ключевой информации не позволит злоумышленнику подобрать ключ, и тем самым обеспечивается безопасность передачи данных. Однако существуют разнообразные атаки, компрометирующие этот протокол [2].

Атака на незащищенную общую точку доступа Wi-Fi

Функциональные возможности многих моделей телефонов позволяют создать Wi-Fi сеть, используя их в качестве точки доступа, что делает устройства уязвимыми для подобного рода атак.

Рассмотрим последовательность действий, выполняемую злоумышленником.

- Поиск и анализ сети

На этом первом шаге атаки нападающий физически обнаруживает сеть, созданную владельцем устройства. Такая операция выполняется с помощью существующих программ сканирования сети (часто используются, например, Netstumbler или Kismet). Анализ пакетов дает злоумышленнику достаточно информации о сети, которая всегда находится в открытом виде, поскольку WEP зашифровывает только часть фреймов данных. Указанные программы позволяют получить следующие данные о сети: SSID, поддерживаемые режимы, флаг с указанием об использовании WEP.

- Соединение с точкой доступа

Если WEP в сети не используется, тогда злоумышленник просто устанавливает SSID.

Некоторые точки доступа позволяют осуществлять доступ к сети только по заранее определенным адресам MAC (физическим адресам).

Для обхода такого рода защиты нападающим используется фальсифицирование MAC-адресов. Для этого злоумышленник дожидается выхода из сети одного из клиентов с известным MAC-адресом. Сам MAC-адрес по сети передается в незашифрованном виде, а значит, при детальном прослушивании может быть вычислен.

- Вторжение в сеть

Результатом атаки может являться получение злоумышленником доступа к общим ресурсам созданной сети, а также подключение к устройствам, входящим в нее, в режиме терминала с целью выполнения на них управляющих команд, что может привести к серьезным последствиям.

Защитой от подобной атаки станет применение шифрования передаваемого по Wi-Fi трафика, что, к сожалению, не гарантирует безопасность сети, но потребует от злоумышленника более высокой квалификации, а также дополнительного времени и средств. В случае передачи информации малой степени важности это может оказаться достаточным для ограждения сети от данной опасности.

Атака на WEP с использованием перехваченных сообщений

Протокол WEP, как уже было сказано ранее, основывается на потоковом шифре RC4. RC4 — вполне надежный алгоритм, но его неправильное использование может привести к появлению уязвимости.

Так, например, основной ошибкой является шифрование двух разных сообщений одним и тем же ключевым потоком.

Рассмотрим пример. Предположим, что открытые тексты P1 и P2 шифруются одним и тем же потоком K.

Тогда верны следующие утверждения:

C1 = P1 xor K

и

C2 = P2 xor K

Но в таком случае также верно следующее:

C1 xor C2 = P1 xor K xor P2 xor K = P1 xor P2

Т. е. злоумышленник, способный перехватить два зашифрованных сообщения, передаваемых по радиоканалу, применив к ним операцию XOR, может получить в свои руки XOR-разность двух открытых текстов.

Если злоумышленник знает хотя бы часть одного открытого текста, он может вычислить и второй, так как реальные сообщения обладают избыточностью, с помощью которой можно извлечь и P1, и P2, имея только P1 xor P2.

Атака на WEP на основе повторного использования ключевого потока

Как было упомянуто выше, ключевой поток в WEP зависит только от **v** и **k**. **k** — фиксированный ключ, который для простоты эксплуатации не меняется часто.

Т. е. ключевой поток зависит только от вектора инициализации **v**, который пересылается по сети в открытом виде. Таким образом, злоумышленник, прослушивая сеть долгое время, может перехватить пакет с уже однажды использованным вектором инициализации.

V имеет длину всего 24 бита. Таким образом, после примерно 16 миллионов пакетов вектор инициализации обязательно будет повторен.

Необходимо также отметить, что длина фиксированного ключа **k** не играет в данном случае никакой роли, так что опасности подвержены как стандартная, так и расширенные реализации WEP.

16 миллионов пакетов для современной беспроводной сети — это не так уж и много, тем более что при осуществлении спланированной и целенаправленной атаки злоумышленник может потратить время на сбор данной информации.

Усугубляется ситуация также тем, что в протоколе не описан алгоритм изменения вектора инициализации **v**, а лишь указана необходимость его вариации.

Многие беспроводные сетевые карты сбрасывают вектор инициализации в 0 при каждом включении и линейно увеличивают его на единицу для каждого последующего пакета. Это значит, что каждая сессия начинается с повторного использования ключевого потока.

Существует множество путей получения текста пакета. Допустим, атакующий знает зашифрованное сообщение **(P)** и открытый текст для некоторых пакетов, зашифрованных с использованием известного вектора инициализации **v**. Тогда он может определить ключевой поток **RC4(k,v)** путем осуществления следующей операции:

(RC4(k,v) xor P) xor P = RC4(k,v)

Злоумышленник не сможет определить ключ **k**, однако он может занести соответствующее ему значение **RC4(k,v)** в таблицу для заданного вектора инициализации **v** и в следующий раз, когда он перехватит пакет с таким же **v**, применить операцию XOR и прочитать данные.

Кроме того, в реализации WEP с ключом в 40 бит нападающий может попытаться напрямую взломать ключ, применив современные вычислительные ресурсы. Очевидно, что расширенный вариант WEP с ключом в 104 бита хотя и усложняет эту задачу, не обеспечит защиты от «атаки по словарю», так как размер словаря будет тот же — вектор инициализации в обоих вариантах имеет размер 24 бита.

Таким образом, из-за некорректной реализации WEP-протокола появляется угроза перехвата и расшифровки Wi-Fi трафика, который может содержать в том числе и важные персональные данные: пароли, конфиденциальные документы, банковскую информацию.

Атака обхода аутентификации WEP

WEP имеет еще одну весомую уязвимость, которая позволяет злоумышленнику осуществлять гораздо более опасные атаки.

Протокол аутентификации, как уже было сказано, создан для проверки того, что клиент знает секретный ключ **k** и может работать в беспроводной сети. Схема указанной операции приведена на рис. 2.

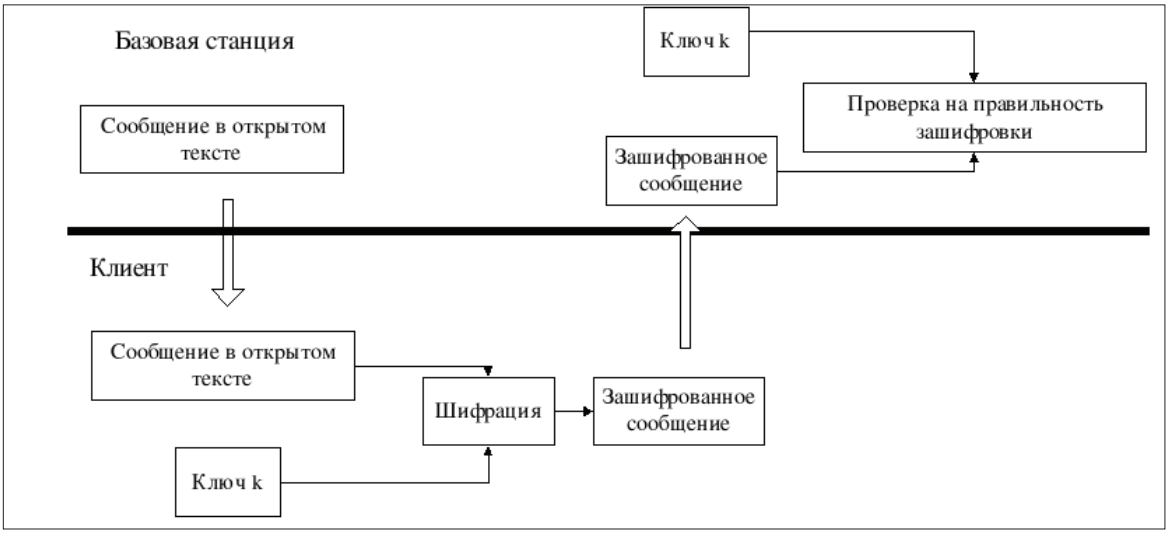

Рис. 2. Схема аутентификации WEP

Выполняются следующие действия:

- точка доступа передает клиенту сообщение (запрос) открытым текстом;
- клиент шифрует его на ключе **k** и отправляет обратно (обычное WEP-шифрование);
- точка доступа проверяет правильность шифрования, используя имеющийся у нее ключ **k**, и в случае успеха аутентифицирует клиента.

Таким образом, если злоумышленнику удастся перехватить пару открытый текст (запрос) / зашифрованный текст (ответ клиента), он не только получит возможность проводить вышеописанные атаки (внедрять пакеты), но и может осуществить нападение на протокол аутентификации, выдав себя за легитимного клиента.

Алгоритм действий атакующего в данном случае выглядит следующим образом.

- Получив открытый и зашифрованный текст, злоумышленник извлекает из сообщения **v** и **RC4(v,k)** с помощью описанных в предыдущей атаке операций.
- После этого злоумышленник пытается внедриться в сеть, выдавая себя за легитимного клиента. Базовая станция посылает ему сообщение **M'**.
- Злоумышленник отвечает передачей следующих данных: вектора инициализации **v** и сообщения, представленного в виде: **<M', c(M')> xor RC4(v,k).**
- Это корректный ответ, и базовая станция принимает злоумышленника, хотя он никогда не знал ключ **k**.

В результате злоумышленник может стать легитимным членом даже защищенной с помощью шифрования сети, тем самым получив доступ к ее ресурсам и устройствам, подключенным к ней.

Атаки отказа в обслуживании Wi-Fi

Цель любой атаки типа отказ в обслуживании состоит в создании помехи при доступе пользователя к сетевым ресурсам. Стандартные методы инициирования атаки заключаются в посылке огромного количества фиктивных пакетов, заполняющих легальный трафик и приводящих к зависанию систем.

Беспроводные системы особенно восприимчивы к такого рода атакам из-за путей, по которым различные уровни OSI стека взаимодействуют между собой.

Атака на физический уровень в беспроводной сети представляет большую опасность ввиду простоты реализации, чем в проводной сети, так как среда передачи данных в этом случае является гораздо менее ограниченной в пространстве.

Также достаточно трудно доказать сам факт проведения атаки отказа в обслуживании на физическом уровне в беспроводной сети.

Например, нападение может быть осуществлено на уровне среды связи.

Злоумышленник может создать устройство, заполняющее весь спектр на частоте 2,4 ГГц, на которой работают беспроводные сети стандарта 802.11b, помехами и нелегальным трафиком — такая задача не вызывает особых трудностей. Даже некоторые недорогие домашние радиотелефоны могут вызывать помехи в указанном диапазоне.

Задачи шифрования и аутентификации позволяет решить, например, такой стек протоколов, как IPSec, который функционирует на сетевом уровне модели OSI. IPSec использует шифр DES для кодирования пакетов и алгоритмы хеширования MD5 и SHA1 для поддержки аутентификации.

Поскольку заголовки транспортного уровня остаются недоступными, пакеты, защищенные с помощью IPSec, не могут преодолевать сетевые экраны. Другой проблемой является необходимость реализации механизмов контроля доставки на сетевом уровне, поскольку транспортный протокол TCP остается недоступным для маршрутизации до получения пакета адресатом. Тем не менее IPSec является обязательной составляющей стандарта IPv6.

Решить перечисленные проблемы и сохранить высокий уровень безопасности позволяет технология SSL, созданная компанией Netscape Communications и перешедшая в стандарт TLS [1].

SSL, в отличие от IPSec, функционирует на 4-м, или транспортном, уровне модели OSI. Эта технология де-факто является стандартом защищенного обмена в Интернете, для ее развертывания создана инфраструктура из сертификационных центров и защищенных веб-сайтов. Также SSL используется и с другими протоколами уровня приложений: с помощью данной технологии защищается пересылка почты, некоторые протоколы обмена мгновенными сообщениями, клиенты интернет-банков и другие приложения.

Интеграция технологий IPSec и SSL/TLS в мобильные платформы и их принудительное использование для всех интерфейсов позволят решить перечисленные проблемы безопасности беспроводной связи.

СПИСОК ЛИТЕРАТУРЫ:

1. *Jahanzeb K.* Building Secure Wireless Networks with 802.11. Wiley, 2003. — 352 с.
2. *Prabhaker M.* Hacking Techniques in Wireless Networks. Dayton, Ohio: Department of Computer Science and Engineering — Wright State University, 2005.