

УДК 004.056

Белорусов Дмитрий Иванович
 Корешков Михаил Сергеевич
 ООО «РИКОМ» г.Москва

E-mail: belorусov@rusmonitor.ru; koreshkovms@rusmonitor.com

WiFi-сети и угрозы информационной безопасности

WiFi-СЕТИ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассмотрены прямые и косвенные угрозы информационной безопасности, которые возникают в связи с развитием технологии беспроводного доступа WiFi. Показано, что применение технологии WiFi может угрожать не только информации, передаваемой непосредственно с помощью оборудования WiFi, но и речевой информации на объекте.

КЛЮЧЕВЫЕ СЛОВА:

WiFi, угрозы, защита информации, информационная безопасность, IEEE 802.11, WEP, WPA, несанкционированный доступ, несанкционированное использование, радиомикрофон

Широкое применение сетей беспроводной передачи данных на основе технологии IEEE 802.11, более известной как WiFi, не может не обращать на себя внимание специалистов по информационной безопасности объектов. В этой статье авторы ставят целью познакомить читателей с результатами исследований новых угроз информационной безопасности объекта, которые связаны с WiFi-сетями.

Изначально технология WiFi была ориентирована на организацию точек быстрого доступа в Интернет (hotspot) для мобильных пользователей. Технология позволяет обеспечить одновременный доступ большого числа абонентов к сети Интернет прежде всего в общественных местах (аэропорты, рестораны и т.д.). Преимущества беспроводного доступа очевидны, тем более что изначально технология WiFi стала стандартом де-факто, и у производителей мобильных компьютеров не возникает вопрос совместимости точек доступа и

мобильных устройств.

Постепенно сети WiFi распространились и на крупные и мелкие офисы для организации внутрикорпоративных сетей или подсетей.

Одновременно с этим крупные операторы связи начали развивать собственные сервисы по предоставлению платного беспроводного доступа в Интернет на основе технологии WiFi. Такие сети состоят из большого числа точек доступа, которые организуют зоны покрытия целых районов городов, подобно сотовой связи.

Как следствие в настоящее время в любом крупном городе рядом практически с любым объектом расположено как минимум несколько WiFi-сетей со своими точками доступа и клиентами, число которых может доходить до сотен.

Перейдем к рассмотрению угроз информационной безопасности, которые возникают в связи с использованием WiFi-сетей. Все угрозы можно условно разделить на два класса:

- прямые - угрозы информационной безопасности, возникающие при передаче

информации по беспроводному интерфейсу IEEE 802.11;

- косвенные — угрозы, связанные с наличием на объекте и рядом с объектом большого количества WiFi-сетей, которые могут использоваться для передачи информации, в том числе и полученной несанкционированно.

Косвенные угрозы актуальны абсолютно для всех организаций, и, как будет показано далее, они представляют опасность не только для информации, обрабатываемой в компьютерных сетях, но и, что наиболее важно, для речевой информации.

Рассмотрим прямые угрозы.

Для организации беспроводного канала связи в технологии WiFi используется радиointерфейс передачи данных. Как канал передачи информации он потенциально подвержен несанкционированному вмешательству с целью перехвата информации, искажения или блокирования.

При разработке технологии WiFi учтены некоторые вопросы информационной безопасности, однако, как показывает практика, недостаточно.

Многочисленные «дыры» в безопасности WiFi дали начало отдельному течению в отрасли компьютерного взлома, так называемому вардрайвингу (*wardriving* – *англ.*). Вардрайверы – это люди, которые взламывают чужие WiFi-сети из «спортивного» интереса, что, однако, не умаляет опасность угрозы.

Хотя в технологии WiFi и предусмотрены аутентификация и шифрование для защиты трафика от перехвата на канальном уровне, эти элементы защиты работают недостаточно эффективно.

Во-первых, применение шифрования снижает скорость передачи информации по каналу в несколько раз и, зачастую, шифрование умышленно отключается администраторами сетей для оптимизации трафика. Во-вторых, использование в WiFi-сетях достаточно распространённой технологии шифрования WEP давно было дискредитировано за счёт слабых мест в алгоритме распределения ключей RC4, который используется совместно с WEP. Существуют многочисленные программы, позволяющие подобрать «слабые» WEP-ключи. Эта атака получила название FMS по первым буквам инициалов разработчиков. Каждый пакет,

содержащий слабый ключ, с 5%-ной степенью вероятности восстанавливает один байт секретного ключа, поэтому общее количество пакетов, которое атакующий должен собрать для реализации атаки, зависит в первую очередь от степени его везучести. В среднем для взлома требуется порядка шести миллионов зашифрованных пакетов. Хакеры лаборатории Hikari of Dasb0den Labs усилили FMS-алгоритм, сократив количество необходимых пакетов с шести миллионов до 500 тысяч. А в некоторых случаях 40/104-битный ключ взламывается всего с тремя тысячами пакетов, что позволяет атаковать даже домашние точки доступа, не нагружая их избыточным трафиком.

Если обмен данными между легальными клиентами и точкой доступа незначителен или практически отсутствует, злоумышленник может заставить жертву генерировать большое количество трафика, даже не зная секретного ключа. Достаточно просто перехватить правильный пакет и, не расшифровывая, ретранслировать его вновь.

Разработчики оборудования отреагировали вполне адекватным образом, изменив алгоритм генерации векторов инициализации так, чтобы слабые ключи уже не возникали.

В августе 2004 года хакер по имени KogeK продемонстрировал исходный код нового криптоанализатора, взламывающего даже сильные векторы инициализации. Для восстановления 40-битного ключа ему требовалось всего 200 000 пакетов с уникальными векторами инициализации, а для 104-битного - 500 тысяч. Количество пакетов с уникальными векторами в среднем составляет порядка 95% от общего количества зашифрованных пакетов, так что для восстановления ключа атакующему потребуется совсем немного времени.

В новом оборудовании WiFi используется технология WPA – Wi-Fi Protected Access (защищённый Wi-Fi-доступ), где вновь была усилена защищённость беспроводных устройств. На место WEP пришел TKIP (Temporal Key Integrity Protocol - протокол краткосрочной целостности ключей), генерирующий динамические ключи, сменяющие друг друга с небольшим интервалом времени. Несмотря на относительную новизну этой технологии, в комплект некоторых хакерских утилит уже входит специальный модуль, отображающий один из ключей протокола. Для несанкционированного подключения к

точке доступа, защищённой технологией WPA, этого оказалось вполне достаточно.

Стандарт IEEE 802.11i описывает более продвинутую систему безопасности (известна под именем WPA2), основанную на криптоалгоритме AES. Готовых утилит для её взлома в открытом виде пока не наблюдается, так что с этой технологией можно чувствовать себя в безопасности. По крайней мере, какое-то время она продержится.

Угроза блокирования информации в канале WiFi практически оставлена без внимания при разработке технологии, что напрасно. Конечно, само по себе блокирование канала не является опасным, поскольку практически всегда сети WiFi являются вспомогательными, однако блокирование зачастую является лишь подготовительным этапом для атаки man-in-the-middle, когда между клиентом и точкой доступа появляется третье устройство, которое перенаправляет трафик между ними через себя. В этом случае возникает уже не только угроза перехвата информации, но и её искажения. Известны, по крайней мере, несколько обработанных атак на WiFi-сети, связанных с отказом в обслуживании DOS (Denial-of-Service), но в рамках данной статьи мы не будем останавливаться на их рассмотрении, ограничимся лишь констатацией наличия реальных угроз.

Перейдем к рассмотрению косвенных угроз информационной безопасности объекта, которые непосредственно связаны с WiFi-технологией.

Каналы WiFi-сетей являются крайне привлекательными для использования в качестве транспортной инфраструктуры для устройств несанкционированного получения информации по целому ряду причин:

1. Сигналы WiFi-устройств имеют достаточно сложную структуру и широкий спектр, поэтому эти сигналы, а тем более, окружающие устройства WiFi невозможно идентифицировать обычными средствами радиомониторинга.

Как показала практика, уверенное обнаружение сигнала WiFi современными комплексами радиомониторинга в широкой полосе частот возможно только по энергетическому признаку при наличии полос параллельного анализа шириной несколько десятков МГц на скорости не менее 400 МГц/с и лишь в ближней зоне. Сигналы точек доступа, расположенных в дальней зоне, оказываются ниже уровня шумов приёмника.

Обнаружение WiFi-передатчиков при последовательном сканировании узкополосными приёмниками вообще невозможно.

2. Практически на каждом объекте или вблизи него развернуты частные WiFi-сети или WiFi-сети общего пользования. В окружении таких сетей крайне сложно отличить легальных клиентов собственной и соседних сетей от клиентов с возможностями негласного получения информации, что даёт возможность эффективно маскировать несанкционированную передачу информации среди легальных WiFi-каналов.

Передатчик WiFi излучает так называемый «OFDM сигнал». Это означает, что в один момент времени устройство передаёт в одном сигнале, занимающем широкую полосу частот (около 20 МГц) несколько несущих информации - поднесущих информационных каналов, которые расположены так близко друг от друга, что при приёме их на обычном приёмном устройстве, сигнал выглядит как единый «купол». Разделить в таком «куполе» поднесущие и идентифицировать передающие устройства можно только специальным приёмником.

3. В крупных городах сети WiFi общего пользования имеют зону покрытия, достаточную, чтобы гарантировать возможность подключения к ним для передачи информации практически любой точки. Это снимает необходимость использования мобильного пункта приёма информации рядом с объектом, поскольку информация может быть передана несанкционированным устройством через точку доступа общего пользования и далее по сети Интернет в любое место.

4. Ресурсы, которые предоставляют каналы WiFi-сетей, позволяют передавать звук, данные, видео в реальном масштабе времени. Этот факт открывает широкие возможности перед устройствами перехвата информации. Теперь не только звуковая информация, но и видеоданные с компьютеров или локальной сети под угрозой.

Все рассмотренные выше преимущества WiFi-технологии с точки зрения защиты информации на объекте являются недостатками. Кроме того, выпускаются и абсолютно легально продаются малогабаритные WiFi-устройства, позволяющие передавать данные, голосовую или видеoinформацию, например, беспроводные WiFi-видеокамеры, которые

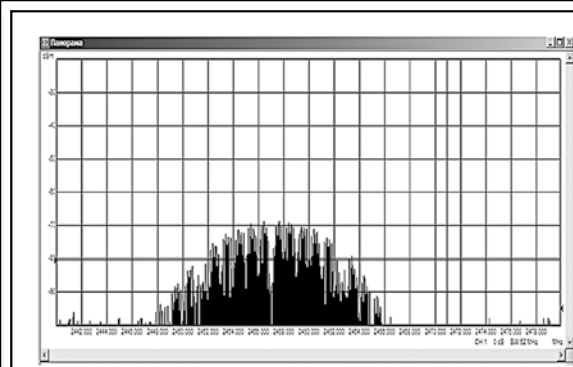


Рис. 1. Сигнал WiFi-передатчика в ближней зоне



Рис. 2. Беспроводная WEB-камера с WiFi-интерфейсом

легко могут быть переделаны для использования в качестве устройств негласного получения информации.

Далее рассмотрим практические реализации косвенных угроз на реальных примерах использования каналов WiFi-устройствами несанкционированного получения информации.

1. В помещении несанкционированно установлена WiFi-видеокамера с микрофоном. Для увеличения дальности передачи информации на крыше объекта устанавливается точка доступа WiFi, которая работает в режиме ретранслятора (один из штатных режимов работы WiFi точки доступа) с направленной антенной. В этом случае информация из помещения, в котором установлена камера стандартной мощности WiFi клиента, может быть принята на контрольном пункте, расположенном на расстоянии нескольких километров от объекта, даже в условиях города.

2. Смартфон одного из сотрудников предприятия с помощью специальной программы

(вируса) может переводиться в режим, когда речевая информация с микрофона будет записываться и с помощью встроенного в него WiFi-модуля передаваться на контрольный пункт.

Для повышения скрытности контрольный пункт может быть использован также в одном из штатных режимов WiFi точек доступа - «передача со скрытым именем». В таком случае точка доступа будет не видима программам обзора сетевого окружения для беспроводных сетей. Необходимо отметить, что в этих программах WiFi клиенты вообще никогда не видны.

3. И, наконец, рассмотрим вариант, когда режим на объекте не позволяет выносить носители информации за его пределы, выход в Интернет отсутствует или ограничен. Как злоумышленник может передать с такого объекта достаточно большой объём данных незаметно? Ответ: ему необходимо абсолютно легально подключиться к соседней широкополосной WiFi-сети и передать информацию, оставаясь

www.rusmonitor.ru

Комплекс мониторинга WiFi и Bluetooth

ЗОДИАК

ЭВРИКА

Комплекс радиоконтроля

РИКОМ

 A promotional banner for radio monitoring software. It features a spectrum analyzer screenshot with a white signal trace on a dark background. The x-axis is labeled 'MHz' and ranges from 400.000 to 720.000. The y-axis shows signal levels. The text 'Комплекс мониторинга WiFi и Bluetooth' and 'ЗОДИАК' is at the top right. 'ЭВРИКА' and 'Комплекс радиоконтроля' is at the bottom right. The website 'www.rusmonitor.ru' is on the left, and the 'РИКОМ' logo is at the bottom left.

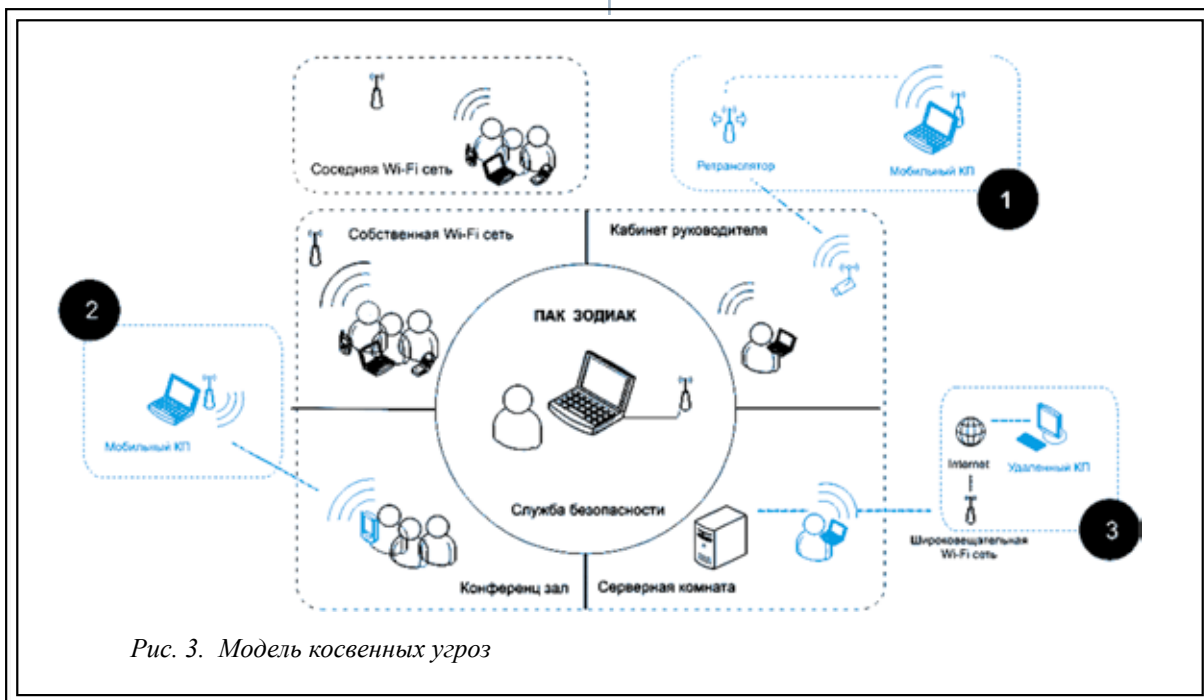


Рис. 3. Модель косвенных угроз

незамеченным среди достаточно большого количества WiFi клиентов соседних сетей, передающих информацию за пределами объекта.

Выводы:

Технология WiFi безусловно удобна и универсальна для организации беспроводного доступа к информации. Однако она несёт в себе множество серьёзных угроз информационной безопасности объекта. При этом существуют прямые и косвенные угрозы информационной безопасности. И если от прямых угроз можно избавиться, отказавшись от применения WiFi-устройств в инфраструктуре корпоративной сети и не использовать WiFi-сети на объекте, то косвенные угрозы существуют независимо от применения на объекте WiFi-технологии. Кроме того косвенные угрозы опаснее прямых, поскольку им подвержена не только информация в компьютерных сетях, но и речевая информация на объекте.

В заключение хотелось бы отметить, что WiFi-технология в настоящее время является не единственной распространённой беспроводной технологией передачи данных, которые могут нести в себе угрозы информацион-

ной безопасности объекта.

Bluetooth-устройства также могут использоваться для организации несанкционированной беспроводной передачи данных. По сравнению с WiFi-у Bluetooth-устройств существенно меньше возможностей с точки зрения дальности передачи информации и пропускной способности канала, но есть одно важное преимущество — низкое энергопотребление, что для несанкционированного передатчика является крайне важным.

Ещё одна технология, которая начинает конкурировать с WiFi при обеспечении беспроводного широкополосного доступа, это - WiMAX. Однако по состоянию на настоящий момент WiMAX - устройства гораздо менее распространены, и их наличие скорее окажется демаскирующим фактором, чем скроет несанкционированный канал передачи информации.

Таким образом, именно WiFi в настоящее время является не только самой распространённой технологией беспроводного доступа, но и самой удобной с точки зрения несанкционированного получения и передачи информации.

Литература

1. Каролик А., Касперски К. Разберемся, что такое вардрайвинг (wardriving) и с чем его необходимо употреблять //Хакер. - №059. - С. 059-0081. <http://www.xakep.ru/magazine/xs/059/008/1.asp>