Для цитирования: Витомский Е.В., Сомов Д.Н. Методы защиты локальной беспроводной сети, направленные на обеспечение временной скрытности сигналов и структуры информационного взаимодействия // Вопросы радиоэлектроники. 2020. № 3. С. 35–40.
DOI 10.21778/2218-5453-2020-3-35-40
УДК 004:056

Е.В. Витомский[1], Д.Н. Сомов[1]

[1] Московский авиационный институт (Национальный исследовательский университет)

МЕТОДЫ ЗАЩИТЫ ЛОКАЛЬНОЙ БЕСПРОВОДНОЙ СЕТИ, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВРЕМЕННОЙ СКРЫТНОСТИ СИГНАЛОВ И СТРУКТУРЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Работа посвящена проблеме безопасности беспроводных локальных сетей. Известно, что против ряда типовых атак самые распространенные сети стандарта IEEE 802.11 плохо защищены. Разрешить эту проблему с помощью штатного программного обеспечения беспроводных устройств получается недостаточно эффективно, а против некоторых атак не представляется возможным. Одной из причин, затрудняющих решение данной проблемы, является низкий уровень временной и пространственной скрытности работы стандартной беспроводной сети. На основе анализа распространенных атак на Wi-Fi-сети разработаны оригинальные методы защиты, учитывающие данный аспект. Разработанные методы воплощены в реальном устройстве. Методы защиты реализованы путем незначительной модификации штатного программного обеспечения устройства, имеющего открытую аппаратную платформу. С участием этого устройства был проведен эксперимент, подтвердивший возможность развертывания локальной беспроводной сети, защищенной с использованием методов, предлагающихся в данной работе.

Ключевые слова: *беспроводные сети, инфокоммуникации, информационная безопасность, протоколы, методы защиты*

Введение

В настоящее время локальные беспроводные сети используются как в домах, так и в торговых центрах, промышленности, офисных зданиях и государственных организациях [1, 2]. Реализуются как публичные, открытые сети, так и закрытые, приватные сети для ограниченного круга пользователей (клиентов). Однако существующих методов защиты локальных беспроводных сетей стандарта Wi-Fi, которые описаны в серии стандартов IEEE 802.11 [3], бывает недостаточно. В организациях, работающих с конфиденциальной информацией, утечка данных из сети – недопустимое событие. Локальные беспроводные сети, развернутые внутри таких организаций, должны быть хорошо защищенными от несанкционированного доступа и отказоустойчивыми. Таким образом, актуальны потребности в анализе уровня защищенности сетей, построенных согласно существующим стандартам, а также в анализе основных уязвимостей таких сетей и типичных атак, проводимых против них. Некоторые производители беспроводных устройств реализуют в своих продуктах варианты защиты от ряда известных атак. Однако в открытых источниках нет достоверной информации о методах, способах реализации и оценках эффективности таких устройств.

Анализ атак, обусловленных недостаточными уровнями пространственной и временной скрытности работы беспроводной локальной сети

Типичная локальная беспроводная сеть состоит из клиентов, оснащенных радиомодулем Wi-Fi, и беспроводной точки доступа. Точка доступа, согласно существующим стандартам, постоянно показывает свое присутствие в сети отсылкой так называемых beacon-пакетов. Эти служебные пакеты содержат данные о режимах и качестве обслуживания в сети точки доступа, уровне сигнала, а также информируют клиента, что рядом имеется такая точка доступа, передают ее название и MAC-адрес. Согласно стандарту 802.11, считается, что наличие beacon-пакетов в радиоэфире позволяет клиентам и другим устройствам, работающим в одном радиоканале, обнаружить корректно работающие точки доступа. При этом не соблюдается временная скрытность точки доступа [4] – ее можно обнаружить в любое время с момента включения и до выключения излучения.

Также по умолчанию беспроводная точка доступа не делает различий между клиентами по уровню их сигнала, и вещание происходит на одинаковой мощности, зачастую избыточной. Частично данная ситуация исправляется ручной корректировкой мощности, но невозможно учесть нужды всех клиентов беспроводной сети, тем более, что клиенты могут перемещаться относительно точки доступа, и в некоторый момент времени мощности отрегулированной точки доступа будет не хватать для поддержания соединения с ними. Динамическое ограничение по сигналу вещания для каждого из клиентов было бы необходимым и достаточным для обеспечения пространственной скрытности точки доступа, но такой функционал, согласно стандарту, не реализован в протоколах 802.11. Постоянство уровня сигнала работающей точки доступа позволяет злоумышленнику иметь больше возможностей по размещению устройств для обнаружения и атаки беспроводных сетей [4].

Авторами был проведен анализ атак, направленных на беспроводные локальные сети, требующих для успешной реализации предварительного получения информации о клиентах и точках доступа в составе сети. Рассмотрим атаки, которые могут быть осуществлены в локальных беспроводных сетях при отсутствии достаточной пространственной и временной скрытности сигналов.

Первый тип – атака типа «отказ в обслуживании». Перехваченные в радиоэфире beacon-пакеты могут дать злоумышленнику достаточно информации о беспроводной точке доступа поблизости и качестве ее сигнала. Тем более, что beacon-пакеты передаются всегда, когда беспроводная точка доступа активна – данное поведение четко регламентировано спецификацией IEEE 802.11. Этот факт делает beacon-пакеты самым опасным фактором нарушения временной и – косвенно – пространственной скрытности устройства в радиоэфире. С использованием специализированных средств, таких как Wi-Fi-адаптеры с более качественными антеннами и высокими параметрами чувствительности приемника (мощности передатчика), способные производить прослушивание эфира, а также специальных утилит для работы с подобными беспроводными адаптерами, достаточно перехватить несколько beacon-пакетов, после чего атака типа «отказ в обслуживании» становится возможной, поскольку хорошо известны параметры точки доступа. При воздействии данной атаки точка доступа становится не способна обслуживать легитимных клиентов или ее пропускная способность значительно снижается [5].

Второй тип – атака типа «спуфинг»: подмена легитимной точки доступа с использованием специализированных средств. Перехват beacon-пакетов или пакетов probe response позволяет узнать подробную информацию о перспективах взаимодействия беспроводной точки доступа с клиентами сети по радиоканалу. Клиенты сканируют сеть, используя пакеты probe request, запрашивая подтверждение на подключение у активных точек доступа в радиусе радиовидимости. Точки доступа должны всегда отвечать пакетами probe response, даже если адрес назначения пакета probe request был широковещательным, т.е. пакет не предназначался именно данной точке доступа. Такое поведение также предустановлено спецификацией. К сожалению, при этом злоумышленнику довольно легко узнать данные точки доступа, с которой пытается общаться клиент, а именно ее идентификатор SSID и MAC-адрес, и с помощью особых утилит сделать так, чтобы его Wi-Fi-адаптер, с точки зрения клиентов сети, стал той беспроводной точкой доступа, пакеты которой были перехвачены. Активность точки доступа подавляется направленной атакой типа «отказ в обслуживании». Таким образом, происходит «подмена» легитимной точки доступа на устройство злоумышленника [6].

Третий тип – несанкционированный доступ в беспроводную сеть. Данная атака может быть следствием перехвата вышеупомянутых beacon-пакетов, слежением за диалогами точек доступа и клиентов и, наконец, перехватом так называемого 4-way handshake – особой последовательности пакетов, которая пересылается в радиоканале при аутентификации клиента в беспроводной сети. Данная последовательность содержит пароль от беспроводной сети в виде hash-кода. Успешная расшифровка возможна только в том случае, если вся последовательность из четырех пакетов будет перехвачена корректно и желательно несколько раз [7]. Это условие для атаки на хеш-функцию парольной фразы обычно легко выполнимо, поскольку зона с высоким уровнем сигналов сети жертвы обладает достаточным постоянством во времени и пространстве, чтобы злоумышленник мог надежно захватить пакеты аутентификации при каждой попытке подключения клиента к точке доступа, находясь достаточно далеко от устройств.

Выявление факторов недостаточной пространственной и временной скрытности работы беспроводной сети

Представленные выше результаты анализа атак, обусловленных легкостью перехвата в радиоэфире пакетов клиентов и точки доступа, указывают на недостаточную скрытность этих устройств и заставляют задуматься о нескольких факторах передачи пакетов. Необходимо учитывать, как минимум, три нижеприведенных аспекта для обеспечения скрытности локальной беспроводной сети.

Во-первых, в беспроводной локальной сети не должно быть избыточных пакетов, однозначно демаскирующих присутствие беспроводной точки доступа. К ним относятся в первую очередь beacon-пакеты точки доступа, а также пакеты probe response, которые точка доступа отправляет как ответы на пакеты probe request от любых клиентов [8, 9].

Во-вторых, в беспроводной локальной сети необходимо иметь возможность защищаться от атак, которые являются достаточно простыми по своей организации, но разрушительными по воздействию на процесс передачи данных в сети. К ним относится, например, атака типа «отказ в обслуживании» с помощью отправки пакетов деаутентификации. Сложно представить себе ситуацию, при которой требуется отключить клиентов от точки доступа ничем не защищенной командой, передаваемой именно по беспроводному каналу.

В-третьих, в беспроводной локальной сети необходимо ограничивать мощность радиоизлучения, которая используется при отправке пакетов, чтобы наличие сети не было заметно за пределами некоторого пространства, внутри которого гарантированно не может быть злоумышленника, который бы смог подслушать трафик и провести на его основе атаку. Пакеты аутентификации и ассоциации не должны передаваться сигналами с избыточной мощностью, так как они содержат важную информацию, такую как хеш-функции парольной фразы.

Метод повышения временной скрытности работы беспроводной точки доступа. Ограниченная отправка широковещательных пакетов

Пусть имеется точка доступа в беспроводной локальной сети и несколько клиентов. Клиентам заранее известно, что данная точка доступа существует. Список адресов клиентов – так называемый «список доверенных клиентов» – известен точке доступа (со временем может изменяться).

Метод защиты заключается в том, чтобы после включения работающая точка доступа не отправляла beacon-пакеты в радиоэфир ни в одном из каналов. При этом входящий поток management-пакетов просматривается точкой доступа.

Режим работы клиентов может не отличаться от определенного стандартной спецификацией 802.11. В частности, клиенты имеют право производить активное сканирование сети на различных каналах.

Точка доступа постоянно фильтрует пакеты probe request во входящем потоке, которые являются следствием активного сканирования, запускаемого клиентами. У данных пакетов точка доступа проверяет адрес отправителя. Если адрес совпадает с одним из представленных в списке доверенных клиентов, точка доступа начинает отправку beacon-пакетов. Сеанс отправки beacon-пакетов ограничен по времени, достаточному для того, чтобы доверенный клиент смог обнаружить присутствие точки доступа. Таким образом, клиент способен увидеть точку доступа после того, как произвел активное сканирование сети, и выполнить подключение к ней. Спустя короткий промежуток времени точка доступа отключает отправку beacon-пакетов.

Непрекращающаяся отправка beacon-пакетов – это главный демаскирующий фактор для точки доступа в локальной беспроводной сети [4]. При этом, чтобы обнаружить стандартную Wi-Fi-точку доступа по beacon-пакетам, злоумышленнику необязательно осуществлять какую-либо активность в данной сети. Рассмотренный же метод защиты может обеспечить практически идеальную временную скрытность точки доступа в периоды отсутствия клиентов.

Метод ограничения доступа недоверенных клиентов к ресурсам точки доступа. Фильтрация входящих пакетов по списку разрешенных адресов

Стандартная точка доступа всегда отвечает пакетом probe response каждому клиенту, который выполняет активное сканирование сети, то есть отправляет пакеты probe request. Метод защиты заключается в том, что на точке доступа так же, как и в предыдущем варианте защиты, имеется список адресов доверенных клиентов сети и производится сканирование входящего потока management-пакетов. При обнаружении во входящем потоке пакета probe request точка доступа обязана проверить его отправителя. Если это не клиент из списка доверенных клиентов, то ответная отправка пакета probe response не производится.

Данный вариант метода защиты является отличным дополнением к способу повышения скрытности с помощью ограничения отправки beacon-пакетов. Был проведен анализ, результаты которого показали, что некоторые продвинутые клиенты (не говоря о специализированном программном обеспечении, которое используют сканеры сети Wi-Fi) отображают точку доступа в списке доступных даже в том случае, когда она не отправляет beacon-пакеты в радиоэфир беспроводной локальной сети. Конечно, это означает, что злоумышленнику придется проявить некоторую активность в сети, иными словами, осуществить активное сканирование, что выдаст его присутствие поблизости, однако раскрытия точки доступа в таком случае можно избежать, применив предлагаемый метод защиты.

Также стоит упомянуть, что фильтрацию входящих пакетов probe request можно реализовать на уровне драйвера устройства, так как

фильтруемые пакеты принадлежат канальному уровню семиуровневой модели OSI [10], в то время как большинство утилит, которые обеспечивают в современных беспроводных точках доступа встроенную функциональность фильтрации по MAC-адресам клиентов, функционируют на седьмом уровне модели OSI – уровне приложений, что делает их гораздо менее эффективными на фоне фильтра канального уровня. Таким образом, экономится значительное количество процессорного времени точки доступа, что косвенно повышает качество обслуживания и снижает энергозатраты.

Метод защиты от DoS-атак

Как указывалось выше, самый простой способ вывести локальную беспроводную сеть из строя – начать продолжительную атаку типа «отказ в обслуживании», основанную на отправке бесконечного потока пакетов деаутентификации и/или деавторизации. Результатом является, во-первых, обрыв сеансов связи между легитимными клиентами и точками доступа, во-вторых – засорение радиоэфира и снижение качества обслуживания.

Метод защиты заключается в том, что все стандартные пакеты деаутентификации и деавторизации игнорируются, не признаются легитимными. Команды на прекращение сеанса между точкой доступа и клиентом, если это необходимо, могут передаваться в data-пакетах только после установленного сеанса связи, вследствие чего они будут защищены шифрованием с помощью стандартных механизмов (например, парольной фразы, которую используют клиент и точка доступа Wi-Fi во время ассоциации и аутентификации).

Следовательно, атака типа «отказ в обслуживании» с помощью отправки пакетов деаутентификации и деавторизации становится полностью невозможной.

Результаты экспериментов

Эксперимент по подтверждению эффективности и достоверности вышеприведенных методов заключался в построении макета беспроводной локальной сети с использованием беспроводной точки доступа, в прошивке которой были реализованы вышеупомянутые модификации. За основу была взята прошивка (программный продукт) с открытым исходным кодом и платформа – сетевое устройство, на которую возможно устанавливать подобные программные продукты. После внедрения модификаций и установки прошивки на платформу (точку доступа) она была протестирована путем включения в макет локальной беспроводной сети, состоящий, помимо точки доступа, из двух клиентских терминалов. Одно из двух устройств играло роль доверенного клиента, второе – недоверенного, т. е. злоумышленника. Следует заметить, что модификация ПО или платформы клиентов не проводилась. Ниже приведены результаты тестирования точки доступа с модифицированной прошивкой.

Тестирование метода «Ограниченная отправка широковещательных пакетов» проведено для двух состояний: доверенный клиент отсутствует в радиусе видимости точки доступа; доверенный клиент присутствует в ее радиусе видимости. В первом варианте было замечено, что, хотя отправка широковещательных пакетов и ограничена, недоверенное устройство могло обнаружить точку доступа только путем активного сканирования. Во второй фазе точка доступа успешно обнаружила доверенного клиента, как только он провел активное сканирование сети, и сопряжение доверенного устройства и точки доступа прошло успешно.

Тестирование метода «Фильтрация входящих пакетов по списку разрешенных адресов» проводилось для тех же двух вариантов состояний совместно с ограниченной отправкой широковещательных пакетов. При отсутствии доверенного клиента в сети недоверенному клиенту не удалось обнаружить точку доступа даже путем активного сканирования сети. К тому же точка доступа оставалась невидимой даже для специализированной аппаратуры (Wi-Fi-адаптеров, способных переходить в режим мониторинга сети). При появлении доверенного клиента обнаружение и сопряжение проходили успешно, однако, после истечения времени отправки широковещательных пакетов на точке доступа недоверенный клиент снова не мог обнаружить точку доступа, так как доверенный клиент больше не запрашивал активное сканирование сети. Это доказывает эффективность совместного использования первых двух методов повышения защищенности.

При тестировании метода защиты от DoS-атак для проведения атаки использовались наиболее распространенные инструменты, такие как утилита aireplay-ng с флагом «-0» (режим деаутентификации). В ходе проведения эксперимента было отмечено, что данная утилита воздействует как на саму точку доступа, так и на ее клиентов. Поэтому хотя на точке доступа и было включено игнорирование фреймов деаутентификации, атака на устройство вызвала отключение всех клиентов, так как им были также отправлены пакеты деаутентификации. На основании данного результата можно сделать вывод, что данный метод способен защитить точку доступа от атак DoS, осуществляемых путем отправки пакетов деаутентификации и деавторизации.

Заключение

Представленные методы защиты беспроводных устройств разработаны против основных

уязвимостей и типичных атак в сетях, построенных согласно спецификациям IEEE 802.11. Они достаточно просто реализуемы на базе открытых аппаратных платформ [11], имеющих в своем составе стандартные адаптеры Wi-Fi, путем небольших модификаций программного обеспечения этих устройств, что подтверждается экспериментально. Еще одним достоинством представленных методов является то, что они могут быть реализованы только на точке доступа, т. е. не нарушают совместимость со штатным оборудованием и программным обеспечением клиентских устройств. На данный момент реализованы первые два метода и частично третий (ограниченная отправка широковещательных пакетов, фильтрация входящих пакетов по списку разрешенных адресов, игнорирование пакетов деаутентификации и деавторизации). Эксперимент с устройством с модифицированным программным обеспечением показал, что производительность беспроводной сети и скорость подключения клиентов в условиях вышеописанных трех типов атак практически не изменялась.

СПИСОК ЛИТЕРАТУРЫ

1. Беспроводные локальные сети в системах промышленной автоматизации [Электронный ресурс]. URL: https://www.bookasutp.ru/Chapter2_11_1.aspx (дата обращения: 06.02.2020).
2. Беспроводные локальные сети Wi-Fi: предназначение и виды [Электронный ресурс]. URL: https://www.sviaz-expo.ru/ru/articles/besprovodnye-lokalnye-seti-wifi (дата обращения: 22.01.2020).
3. IEEE802.11–1999. IEEE Standard for Information technology [Электронный ресурс]. URL: https://standards.ieee.org/standard/802_11–1999.html (дата обращения: 21.01.2020).
4. Смирнова Е. В., Пролетарский А. В. и др. Технологии современных беспроводных сетей Wi-Fi. Москва: Издательство МГТУ им. Н. Э. Баумана, 2017. 448 с.
5. Mohit R. Python penetration testing essentials. 2nd ed. Birmingham, Packt Publishing, 2018. 230 p.
6. Schultz C. P., Perciaccante B. Kali Linux cookbook. 2nd ed. Birmingham, Packt Publishing, 2017. 440 p.
7. How to crack WPA/WPA2 [Электронный ресурс]. URL: https://www.aircrack-ng.org/doku.php?id=cracking_wpa (дата обращения: 21.01.2020).
8. WLAN probe request frame | Probe response frame [Электронный ресурс]. URL: https://www.rfwireless-world.com/Terminology/WLAN-probe-request-and-response-frame.html (дата обращения: 21.01.2020).
9. Gast M. S. 802.11 wireless networks: the definitive guide. 2nd ed. Sebastopol, U.S., O'Reilly Media, 2009. 464 p.
10. Тхи Л. Л., Минь Д. Б. и др. Сетевая модель OSI // Научные исследования. 2017. № 1. С. 15–18.
11. OpenWRT | Wireless freedom [Электронный ресурс]. URL: https://openwrt.org (дата обращения: 21.01.2020).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Витомский Евгений Владиславович, старший преподаватель, Московский авиационный институт (Национальный исследовательский университет), Российская Федерация, 125993, Москва, Волоколамское ш., д. 4, тел.: 8 (916) 950-28-31, e-mail: euvit@ya.ru.

Сомов Дмитрий Николаевич, студент магистратуры, Московский авиационный институт (Национальный исследовательский университет), Российская Федерация, 125993, Москва, Волоколамское ш., д. 4, тел.: 8 (905) 521-49-80, e-mail: 1000lop@gmail.com.

For citation: Vitomsky E. V., Somov D. N. Methods for protecting local wireless network aimed at providing temporary silency of signals and information interaction structure. Issues of radio electronics, 2020, no. 3, pp. 35–40.
DOI 10.21778/2218-5453-2020-3-35-40

E. V. Vitomsky, D. N. Somov

METHODS FOR PROTECTING LOCAL WIRELESS NETWORK AIMED AT PROVIDING TEMPORARY SILENCY OF SIGNALS AND INFORMATION INTERACTION STRUCTURE

This work is devoted to the security problem of wireless local area networks. It is known that against a number of typical attacks, the most common IEEE802.11 networks are poorly protected. Existing ways of solving this problem with the help of regular wireless device software are not effective enough, and against some attacks, it is even not possible. One of the reasons, which complicates the solution of this problem, is low level of temporal and spatial security of modern wireless network. Based on the analysis of common attacks on Wi-Fi networks, original protection methods have been developed to consider this aspect. These methods were embodied in a real device. Protection methods are implemented by slightly modifying the standard software of the device having an open hardware platform. An experiment was carried out using this device, which confirmed the possibility of deploying a local wireless network which security was enhanced using the methods proposed in this paper.

Keywords: wireless networks, info-communications, information security, protocols, protection methods

REFERENCES

1. Wireless LANs in industrial automation systems. Available at: https://www.bookasutp.ru/Chapter2_11_1.aspx (accessed 06.02.2020).

2. Wireless Wi-Fi local networks: purpose and types. Available at: https://www.sviaz-expo.ru/ru/articles/besprovodnye-lokalnye-seti-wifi (accessed 22.01.2020).
3. IEEE802.11–1999. *IEEE Standard for Information technology.* Available at: https://standards.ieee.org/standard/802_11–1999.html (accessed 21.01.2020).
4. Smirnova E. V., Proletarsky A. V., et al. *Tekhnologii sovremennykh besprovodnykh setei Wi-Fi* [Technologies of modern wireless Wi-Fi networks]. Moscow, BMSTU Publ., 2017, 448 p. (In Russian).
5. Mohit R. *Python penetration testing essentials.* 2nd ed. Mohit. Birmingham, UK: Packt Publishing, 2018, 230 p.
6. Schultz C. P., Perciaccante B. *Kali Linux cookbook.* 2nd ed. Birmingham, Packt Publ., 2017, 440 p.
7. How to crack WPA/WPA2. Available at: https://www.aircrack-ng.org/doku.php?id=cracking_wpa (accessed 21.01.2020).
8. WLAN probe request frame | Probe response frame. Available at: https://www.rfwireless-world.com/Terminology/WLAN-probe-request-and-response-frame.html (accessed 21.01.2020).
9. Gast M. S. *802.11 wireless networks: the definitive guide.* 2nd ed. Sebastopol, U.S., O'Reilly Media, 2009, 464 p.
10. Thi L. L., Min D. B. et al. OSI network model. *Nauchnye issledovaniya,* 2017, no. 1, pp. 15–18. (In Russian).
11. OpenWRT | Wireless freedom. Available at: https://openwrt.org (accessed 21.01.2020).

AUTHORS

Vitomsky Evgeny, senior lecturer, Moscow Aviation Institute (National research university), Russian Federation, 125993, Moscow, Volokolamskoe Rd., 4, tel.: +7 (916) 950-28-31, e-mail: euvit@ya.ru.
Somov Dmitriy, graduate student, Moscow Aviation Institute (National research university), Russian Federation, 125993, Moscow, Volokolamskoe Rd., 4, tel.: +7 (905) 521-49-80, e-mail: 1000lop@gmail.com.