ЗАЩИТА ДАННЫХ ПРИ ПЕРЕДАЧЕ ПО БЕСПРОВОДНЫМ КАНАЛАМ СВЯЗИ

А.В. Скрыпников, *д-р техн. наук, профессор*
В.В. Денисенко, *старший преподаватель*
К.С. Евтеева, *магистр*
Воронежский государственный университет инженерных технологий
(Россия, г. Воронеж)

DOI: 10.24411/2500-1000-2019-11485

Аннотация. *Предлагается анализ угроз и способов борьбы с ними для гарантированной и безопасной передачи информации по беспроводным каналам связи. В статье последовательно описываются особенности беспроводный связи, типовые стандарты защиты, их уязвимости, способы обхода методов шифрования, перспективы защиты от популярных методов взлома.*

Ключевые слова: *информационная безопасность, защищенность канала, взлом, перехват, защита, киберугрозы, шифрование, беспроводная связь.*

Беспроводные каналы связи в современной развивающейся информационной среде увеличивают конкуренцию стандартным каналам, обширное признание получили беспроводные сети (WLAN), применение беспроводных технологий может быть превосходной альтернативой, когда прокладка кабеля затруднительна, обходится чересчур дорого или невозможна, в то же время становятся более доступными и технологические методы для перехвата данных в корыстных целях сторонними лицами. Необходимо понять, каково принципиальное отличие данных каналов связи в исследуемом контексте, и почему уязвимы эти способы передачи информации. Эта проблема актуальна для нас сегодня ввиду того, что с 2013 года Россия входит в первую десятку стран по киберпреступлениям.

Многие протоколы шифрования современных систем имеют изъяны, стандартные системы защиты лишь формально работают, не давая полной уверенности в защищённости для рядового пользователя. Если говорить об обычных пользователях, то определено, что средний уровень защищенности находится в диапазоне между 34,11 и 46,8 балла по оценочной 100-балльной шкале [4, с. 70].

Следует отметить, что речь далее будет идти про защиту от намеренного вмешательства. Естественные причины, такие как плохое экранирование приемной аппаратуры, побочные полосы, присутствие отражающих поверхностей, помехи рассматривать не будем [2, с. 494].

Для того чтобы описать способы защиты, ниже опишем принцип работы беспроводный сети, и, следовательно, её уязвимости.

Из-за общедоступного свойства радиоспектра появляются неповторимые проблемы с безопасностью, отсутствующие в проводных сетях. Большая часть вариантов беспроводной сети строится не менее чем из двух обязательных составляющих: точки беспроводного доступа и пользователя беспроводной сети – Hot-spot (существует и режим ad-hoc, где пользователя коммуницируют напрямую друг с другом). В отличие от проводной сети, для подключения не нужно иметь прямой физический доступ к работающему сетевому оборудованию, но достаточно пребывая в приделах радиодоступности наладить логическую связь (ассоциацию) с точкой доступа.

В таких сетях вероятны разные типы защиты, но чаше используется стандарты категории 802.11. Если совсем не использовать методы защиты, то любая станция, работающая по стандарту 802.11 на том же радиодиапазоне может принять транслируемые данные.

Здесь часто применяются протокол WEP (шифрование на основе алгоритма RC4 с ключом из статической и динамической части), протокол WAP (WPA) (даль-

нейшее развитие алгоритма шифрования RC4, где контрольные криптографические суммы в WPA просчитываются по новому методу, который называется MIC (Message Integrity Code)), фильтрация MAC-адресов (формируется таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы).

Для обобщенного описания уровня защищенности при применении того или иного типового метода защиты можно наглядно представить их в виде пирамиды на рисунке 1.

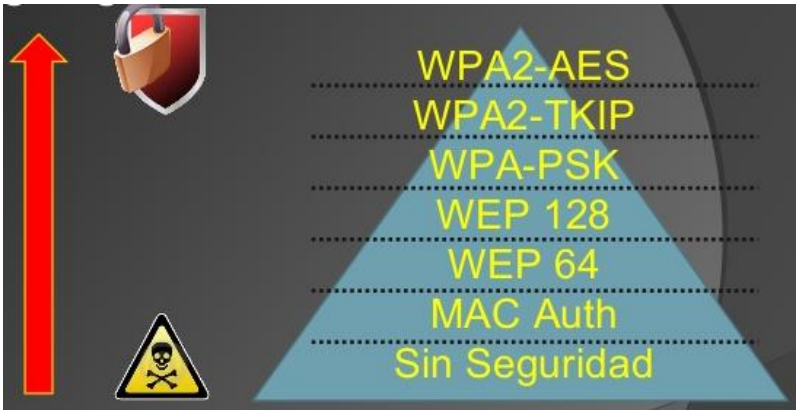

Рис. 1. Пирамида уровней защищенности беспроводных каналов с помощью разных способов

В качестве перспективы для коррекции уязвимостей опишем слабые места перечисленных выше типовых современных способов защиты.

Для обхода протокола безопасности WEP мошенниками используется утилита aircrack 2.4. Для подбора секретного ключа создается специальный ivs-файл. Это только один из примеров, разные программы обращены лишь на определённый перечень чипов, на которых строятся сетевые адаптеры. Количество пакетов, которые нужно изучить для успешного взлома сети, зависит от длины WEP-ключа, часто достаточно захватить полмиллиона пакетов, это может занять не более нескольких минут при интенсивном трафике (рис. 2).

Как видим, обход протокола не требует сверхусилий, и все программы и инструкции есть в свободном доступе.

Обход фильтрации по MAC-адресам. Существуют программы, которые позволяют подменять MAC-адрес сетевого интерфейса, это уже не говоря, что даже с помощью представленной выше утилиты SSID сети можно будет использовать для создания профиля подключения к сети.

Атакующий может применить анализатор протокола для нахождения, санкционированного в BSS MAC-адреса и сетевую карту, пропускающую локальное назначение адреса, для подражания разрешенному MAC-адресу.

Часто используют утилиту SMAC 1.2. В качестве нового MAC-адреса применяется MAC-адрес авторизованного в сети клиента.

Взлом протокола WPA. Осуществляется теми же программами, что и для обхода протокола безопасности WEP, но этот протокол требует существенно большего времени для перебора ключей, в отличие от нескольких минут для WEP, этот протокол требует полной загрузки вычислительных мощностей современных процессоров до нескольких часов (и больше). Результат взлома секретного ключа технически не связан с тем, какой алгоритм шифрования (TKIP или AES) применяется в сети.

Перечислим разные виды атак извне, в том числе те которые описаны выше:

– FMS-атака. Анализ передаваемых векторов инициализации при условии наличия «слабых» инициализационных векторов;

– Атака KOREK’A;

– PTW-атака. Прослушивание большого числа ARP-пакетов;

– Пассивные и активные сетевые атаки;

– Повторное применение вектора инициализации;

– Манипуляция битами;

– Манипуляция с ICV.

Вопросы безопасности в сетях WiMAX, организованных на стандарте IEEE 802.16, также как и в сетях Wi-Fi (IEEE 802.11), также стоят весьма злободневно в связи с простотой подключения к сети.

В сетях LTE алгоритмы шифрования и снабжения общей безопасности созданы на технологии Snow 3G и стандарте AES. Кроме данный двух алгоритмов, технология 3GPP применяет два дополнительных алгоритма таким образом, что даже если один из алгоритмов будет нарушен, оставшиеся должны снабдить безопасность сети LTE.

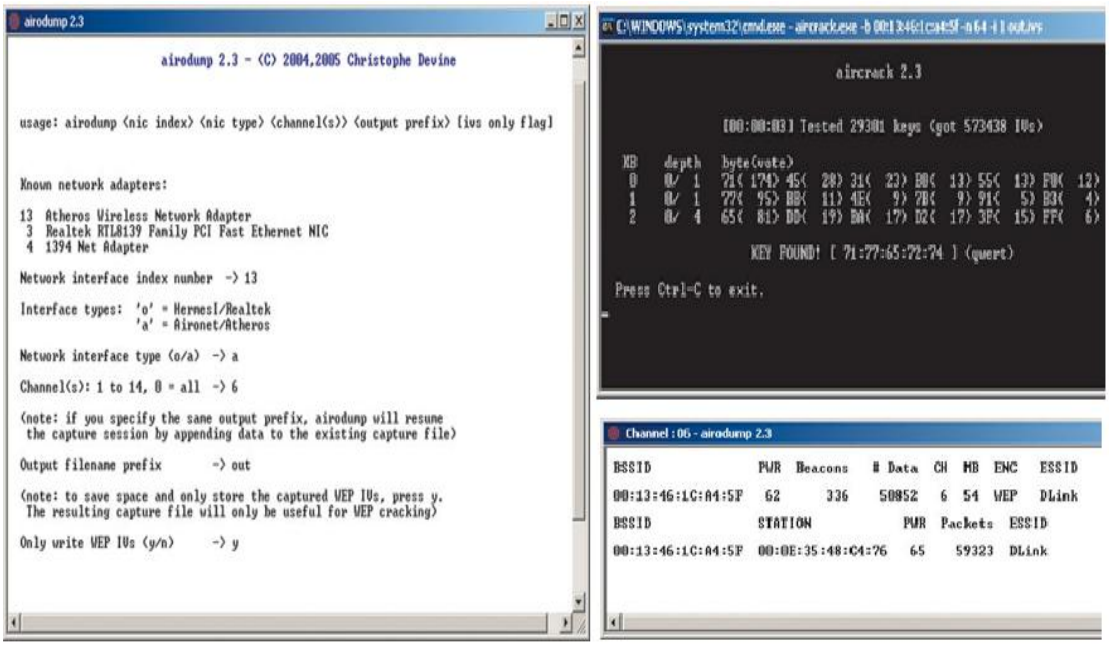

Рис. 2. Иллюстрация обхода протокола безопасности WEP с помощью утилиты airodump

Не стоит забывать, что беспроводные сети можно формально классифицировать на домашние, общедоступные и корпоративные. В каждом из этих случаев есть резон использовать различные подходы к снабжению безопасности сети, так как модели угроз разнятся для каждого из типов сетей. В целом подобных методов очень много, опишем лишь некоторые.

Для защиты корпоративных сетей большой известность пользуются решения на основе технологии 802.1X.

Рядовые пользователи оставляют те же ESSID и протоколы шифрования и аутентификации, которые были введены при производстве, стоит уделить их настройке внимание.

Для создания надежной системы безопасности беспроводных сетей разработано много и других способов. К примеру, достаточно хорошим методом считается применение виртуальных частных сетей VPN (Virtual Private Network). Но VPN присущи изъяны аналогичные криптографическим способам защиты.

Успех взлома секретного WPA-ключа зависит от того, есть он в словаре или нет, поэтому если применять просто набор символов, а не общеупотребляемые слова, то уровень защиты будет увеличиваться экспоненциально, до практически 100% защиты от возможности взлома с помощью подбора.

Для особо важных объектов в виде перспективного направления предлагается применение хаотических широкополосных сигналов. Предлагаемый подход организован на применении перезаписываемых накопителей хаотических рядов, дающих возможность использовать уникальные комплексы хаотических сигналов [1, с. 38].

Можно применять режим скрытого идентификатора SSID, который базируется на том, что для своего обнаружения точка

доступа время от времени транслирует кадры-маячки (beacon frames).

Есть универсальный вариант – это ограничить подверженность разведке и или вовсе устранить угрозу, расположив точку доступа так, чтобы она снабжала нужное покрытие территориально, и это покрытие бы минимально выходило за контролируемую территорию. Нужно настраивать мощность передачи сигнала от точки доступа и применять специальные инструменты для контроля распространения сигнала, специальное глушение сигнала и т.п.

По возможности стоит применить алгоритм шифрования WPA2, алгоритм WEP представляется морально устаревшим. Либо применять в целом стандарт 802.11i, устремленный на рост безопасности беспроводных сетей: он предполагает применение шифрования AES.

Если функциональные возможности точки доступа позволяют запретить ее настройку, используя соединение по радиоканалу – то следует воспользоваться этой функцией.

Заключение. Как видно, современные системы защиты требуют дополнительного внимания в каждом конкретном случае. Для рядового пользователя наиболее простой способ – физически ограничить возможность доступа к беспроводной сети сторонних лиц. Методов оптимизации современных протоколов шифрования достаточно много, как минимум стоит перейти на современные протоколы WPA.

Библиографический список

1. *Жук А.П.,* Осипов Д.Л, Гавришев А.А., Бурмистров В. А. Анализ методов защиты от несанкционированного доступа беспроводных каналов связи робототехнических систем // Наукоемкие технологии в космических исследованиях Земли. – 2016. – №2. – С. 38-42.

2. *Карцан Р.В.,* Карцан И.Н. Беспроводной канал передачи информации, и ее защита // Актуальные проблемы авиации и космонавтики. – 2015. – №11. – С. 494-496.

3. *Абрамов Г.В.,* Денисенко В.В. Моделирование пакетной передачи сети при условии гарантированной доставки // Математические методы в технике и технологиях – ММТТ. – 2014. – № 4 (63). – С. 211-213.

4. *Старцев С.С.* К вопросу защиты беспроводных сетей на базе технологии Wi-Fi // Вестник НГУ. Серия: Информационные технологии. – 2012. – №1. – С. 62-72.

5. *Скрыпников А.В.,* Хвостов В.А., Чернышова Е.В., Самцов В.В., Абасов М.А. Нормирование требований к характеристикам программных систем защиты информации // Вестник Воронежского государственного университета инженерных технологий. – 2018. – Т. 80. № 4 (78). – С. 96-110.

PROTECTION OF DATA WHEN TRANSMITTING WIRELESS COMMUNICATION CHANNELS

A.V. Skrypnikov, *Doctor of Technical Sciences, Professor*
V.V. Denisenko, *Senior Lecturer*
K.S. Evteeva, *Master*
Voronezh State University of Engineering Technologies
(Russia, Voronezh)

Abstract. *The analysis of threats and methods of struggle for guaranteed and safe transmission of information via wireless communication channels is proposed. The article successively describes the features of wireless communications, typical security standards, their vulnerabilities, ways to bypass encryption methods, and the prospects for protection against popular hacking methods.*

Keywords: *information security, channel security, hacking, interception, protection, cyber threats, encryption, wireless communication.*