УДК 004.056

А.С. МАРКОВ, доцент кафедры информационной безопасности
МГТУ им. Н.Э. Баумана, к.т.н.
Ю.В. РАУТКИН, начальник ВП МО РФ 3282, к.т.н.
А.А. ФАДИН, аспирант МГТУ им. Н.Э. Баумана

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ АНАЛИЗА ЗАЩИЩЕННОСТИ WI-FI СЕТЕЙ

Ключевые слова: Wi-Fi сети; аудит безопасности; анализ защищенности; беспроводные сети; IEEE 802.11.

Введение

Одной из базовых технологий развертывания корпоративных сетей в настоящее время является беспроводная сеть Wi-Fi, что стало возможно благодаря ее высокой пропускной способности, надежности, удобству использования и легкости инсталляции [4, 12]. При этом надо понимать, беспроводная среда передачи радиосигнала создает условия для неконтролируемого подключения к сети. Классические способы защиты Wi-Fi сети, заложенные в спецификации ее стандарта, включают в себя шифрование и аутентификацию пользователей [5, 8, 11]. Рассмотрим особенности анализа защищенности Wi-Fi сетей.

Ретроспектива семейства стандартов 802.11

Последним утвержденным стандартом беспроводных сетей Wi-Fi является IEEE 802.11n, вопросы безопасности которого определены спецификацией IEEE 802.11i. Стандарт определил теоретическую скорость передачи данных 540 Мбит/с на рабочих частотах 2,4 и 5 МГц. Ему предшествовали такие стандарты, как IEEE 802.11g (пропускная способность 54 Мбит/с, рабочая частота 2,4 МГц), IEEE 802.11b (пропускная способность 11 Мбит/с, рабочая частота 2,4 МГц), IEEE 802.11a (пропускная способность 54 Мбит/с, рабочая частота 5 МГц). В последующих реализациях стандарта IEEE 802.11 обеспечивается обратная совместимость с ранее принятыми стандартами беспроводных сетей Wi-Fi при условии совпадения диапазона рабочих частот. Например, с версией «a» совместим только стандарт «n». В режиме совместимости со стандартом «b» скорость передачи данных в канале падает до 11 Мбит/с. Кроме диапазона рабочих частот и пропускной способности сети, активно развивались от одной реализации стандарта к другой методы криптографической защиты передаваемой информации и способы аутентификации пользователей. Они прошли ступени развития от открытой системы аутентификации и шифрования канала на основе 24-битового ключа до аутентификации и шифрования на основе 128-битового ключа с помощью алгоритмов AES. При этом аутентификация может быть осуществлена с помощью статического ключа или на основе RADIUS-сервера.

Заметим, в реально существующих беспроводных Wi-Fi сетях одновременно может использоваться оборудование различных версий стандарта [9]. Это оказывает отрицательное влияние не только на общую пропускную способность сети, но и на ее безопасность, поскольку устаревшее оборудование не может поддерживать современные методы обеспечения безопасности. В тех случаях, когда используется современное оборудование,

отрицательное влияние на безопасность может оказать «человеческий фактор». Его проявлениями служат ключи шифрования низкой стойкости, параметры сети, настроенные «по умолчанию», а также устаревшие версии прошивок сетевого оборудования. Рассмотрим некоторые протоколы безопасности.

Протокол WEP

Протокол WEP (Wired Equivalent Privacy) в настоящее время представляет устаревшую спецификацию безопасности Wi-Fi сетей протоколов IEEE 802.11a/b/g. Основными его недостатками являются [1, 2, 3, 7]:

- использование для шифрования непосредственно пароля, введенного пользователем;
- недостаточная длина ключа шифрования;
- использование функции CRC32 для контроля целостности пакетов;
- повторное использование векторов инициализации и др.

На данный момент существует большое количество программ, позволяющих взломать протокол WEP за короткое время (таблица 1).

Протокол 802.1X

Очередным витком развития безопасности беспроводной Wi-Fi сети явилось применение в ней протокола 802.1X. Его суть в том, что вновь подключаемая станция не получает доступа к сети, пока не пройдет процедуру аутентификации. Функции аутентификатора обычно выполняет сервер RADIUS. Основным недостатком, сдерживающим внедрение данного протокола, является необходимость развертывания в сети отдельного сервера аутентификации, что нецелесообразно в малых и средних Wi-Fi сетях.

Таблица 1

Программы взлома протокола WEP

Программа	Реализованные атаки	Время взлома протокола WEP	Год
dwepcrack	Улучшенная FMS	4 ч	2001
AirSnort	FMS	15 ч	2001
AirCrack	Улучшенная FMS, атака Koreka	до 5 мин	2005
WepLab	Улучшенная FMS, атака Koreka	до 5 мин	2005

Стандарт 802.11i и протоколы WPA/WPA2

Рассмотренные недостатки протокола WEP отсутствуют в промежуточном стандарте безопасности 802.11i, который определяет протоколы шифрования WPA (Wireless Protected Access) и WPA2. В отличие от WEP, в WPA/WPA2 реализованы следующие преимущества:

- ключи шифрования генерируются во время соединения (а не распределяются статически);
- для контроля целостности передаваемых сообщений используется алгоритм Michael;
- используется вектор инициализации существенно большей длины.

В данном случае аутентификация пользователей возможна с помощью RADIUS-сервера и введенного заранее ключа. Стандарт IEEE 802.11i обязывает применять алгоритм шифрования AES с использованием режима счетчика и протокола CCMP. Режим счетчика AES — это блочный шифр, за один раз шифрующий 128-битовый блок данных при помощи 128-битового ключа шифрования. Алгоритм CCMP по алгоритму Michael генерирует код целостности сообщений (MIC), обеспечивающий беспроводному фрейму проверку подлинности происхождения данных и их целостность. Ключ шифрования может быть статическим для всей сети (режим PSK) или выдаваться сервером RADIUS (режим EAP). В любом слу-

чае каждый пакет, передаваемый по сети, защищен 128-битовым уникальным ключом, что обеспечивает высокий уровень безопасности.

При использовании протокола WPA2 ключ шифрования отличается не только для различных рабочих станций, но и для различных соединений одной и той же станции.

В настоящее время протокол WPA2 считается надежным, так как нет сколько-нибудь действенного способа его взломать кроме прямого подбора пароля. Поэтому главным условием обеспечения безопасности Wi-Fi сети с протоколом WPA2 является использование надежного пароля. Надежной считается последовательность длиной более 20 произвольных символов (прописные и строчные буквы различных алфавитов, цифры и другие символы). Согласно стандарту 802.11i на каждый символ парольной фразы приходится 2,5 бита ключа безопасности. Парольная фраза из N символов должна порождать ключ безопасности длиной $(2{,}5 * N + 12)$ бит, который, например, будет равен 62 битам при пароле длиной 20 символов. Время для подбора такого ключа несравнимо велико.

Атаки, направленные на пользователей

Развитие протоколов обеспечения безопасности беспроводных сетей заставляет злоумышленников искать обходные пути для их взлома. Наиболее распространенными в данном контексте являются компьютерные атаки, направленные на пользователей Wi-Fi сети.

Можно выделить четыре основные угрозы безопасности, связанные с мобильными клиентами:

• атаки на ОС и прикладное ПО клиентов беспроводной сети;

• перехват трафика при использовании незащищенных беспроводных соединений;

• атаки «человек посередине», которые могут быть использованы для реализации других атак;

• использование беспроводных клиентов в качестве канала удаленного доступа к корпоративной сети.

Для уменьшения вероятности реализации данных атак необходимо:

• постоянно следить за обновлениями операционной системы, драйверов сетевой карты и прошивок точки доступа;

• не использовать незащищенное беспроводное соединение;

• для повышения безопасности связи организовать VPN.

Нерешенные проблемы стандарта 802.11i

Действия злоумышленника могут быть направлены также на вывод беспроводной Wi-Fi сети из строя. Этому могут способствовать нерешенные проблемы, в частности протокола безопасности IEEE 802.11i. Ими являются, например:

• возможность проведения атаки на отказ в обслуживании на физическом уровне (путем глушения радиосигнала) или на канальном уровне (путем эксплуатации уязвимости метода доступа к несущей);

• реализация функции энергосбережения (легальный пользователь может не получить предназначавшейся ему информации при выходе из режима ожидания);

• наличие уязвимости протокола аутентификации EAP (позволяет послать клиенту ложные фреймы успешной аутентификации или отсоединения от сети) и др.

Исследования защищенности Wi-Fi сетей

Для определения реального состояния уровня безопасности беспроводных Wi-Fi сетей были проведены множественные исследования по защищенности реальных беспроводных сетей. Результаты отразили основную тенденцию: несмотря на стремительные темпы развития средств обеспечения безопасности беспроводных сетей Wi-Fi, многие пользователи данных сетей продолжают применять в работе устаревшие методы криптозащиты либо не используют их вовсе (рис. 1 и 2).

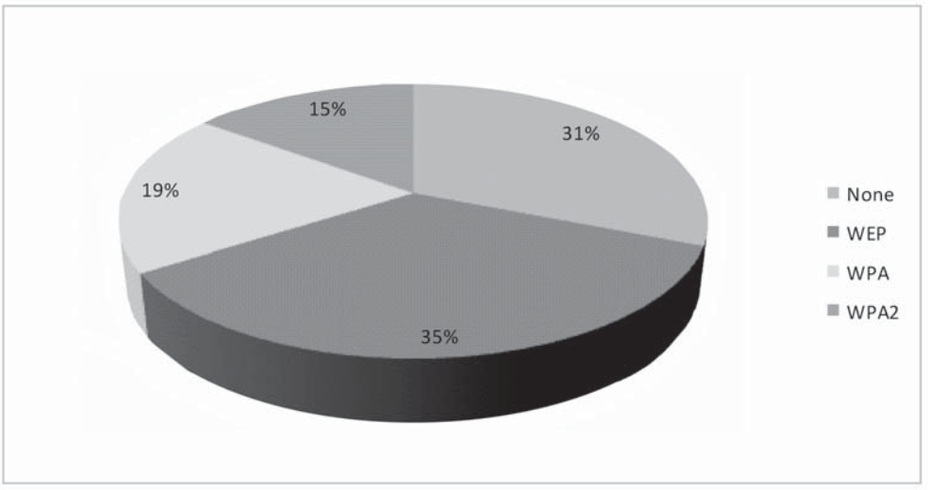

Рис 1. Используемые протоколы защиты Wi-Fi сетей.

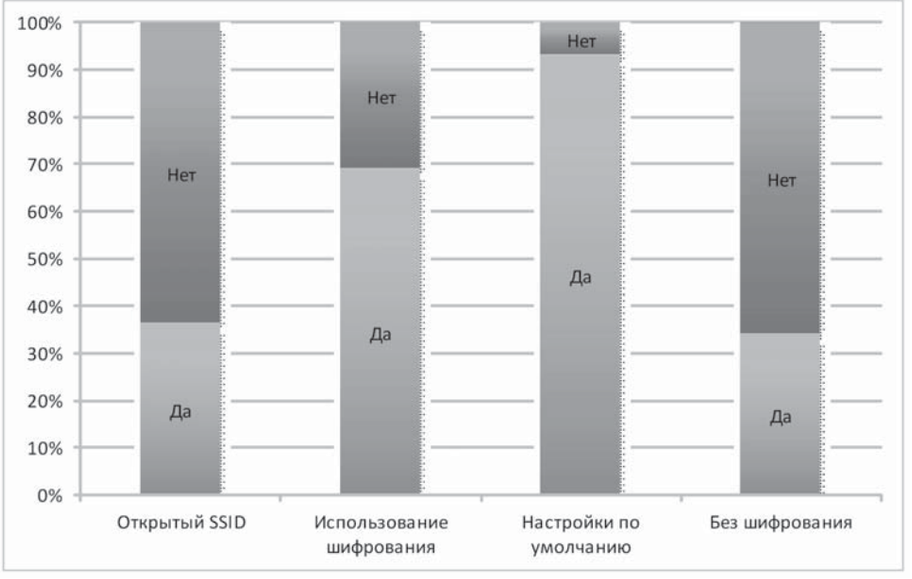

Рис 2. Показатели защищенности беспроводной сети.

Причинами нарушений являются:

• использование устаревшего оборудования;

• использование необновленного программного обеспечения точек доступа или устаревших драйверов сетевых карт;

• использование настроек по умолчанию при конфигурации беспроводной Wi-Fi сети;

• конфигурация беспроводной Wi-Fi сети без учета современных требований безопасности, например: использование алгоритма шифрования WPA2, использование стойкого ключа шифрования, изменение SSID сети «по умолчанию», фильтрация пользователей сети по MAC-адресу.

Методики взлома, используемые злоумышленниками

На практике злоумышленники выполняют взлом Wi-Fi сетей, основанный на эксплуатации уязвимостей различных алгоритмов, протоколов, версий программного обеспечения, он может быть выполнен с помощью различных инструментальных средств (таблица 2). Абсолютное большинство из них являются программами с открытым кодом, функционирующими в ОС семейства Linux. Этому есть ряд объективных причин. Во-первых, данное программное обеспечение легко оптимизируется для выполнения конкретной задачи, во-вторых, ОС семейства Linux позволяют проводить более гибкую настройку сетевого оборудования, которое предстоит использовать для атаки на сеть.

Таблица 2

Программы для взлома Wi-Fi сетей

Программа	Реализованные возможности
Netstumbler 0.4.0	Сбор данных
Kismet	Сбор данных, сохранение сетевого потока в файл
Airtraf, Gtkskan, AirFart	Обнаружение сетей
Aircrack-NG	Сбор данных, атака на сеть, сохранение сетевого потока

Процесс взлома безопасности Wi-Fi сети согласно решаемым задачам целесообразно разбить на следующие этапы:

1) конфигурирование беспроводных карт и интерфейсов;

2) осмотр и нанесение на карту доступных беспроводных сетей (сбор данных);

3) проведение непосредственно атаки на сеть.

Моделирования действий нарушителя как метод аудита

Анализ защищенности Wi-Fi сети, как и взлом, преследуя различные цели, имеет единый подход, поэтому может основываться на тщательном анализе возможных действий злоумышленников, направленных на реализацию различных угроз нарушения безопасности.

Используя комбинации имеющихся уязвимостей и недостатки в конфигурации сети и применяемой политике безопасности, нарушители (как внешние, так и внутренние) в зависимости от своих целей реализуют разнообразные стратегии нападения. Эти стратегии могут быть направлены на различные критические ресурсы сети и включать многошаговые цепочки атакующих действий. В рамках этих цепочек может осуществляться компрометация различных сетевых устройств и реализация различных угроз безопасности.

Высокая сложность Wi-Fi сетей и механизмов защиты (возможность использования различных методов аутентификации и шифрования), увеличение количества уязвимостей и потенциальных ошибок в их использовании, а также возможностей по реализации атак обусловливают необходимость разработки средств автоматизации анализа защищенности.

Средства автоматизации анализа защищенности могут реализовывать активные методы анализа уязвимостей. Активные методы основываются на «тестировании сетей на проникновение», которое выполняется путем реализации различных атакующих действий [6, 10].

Анализируя процесс взлома и проецируя его в область аудита Wi-Fi сетей, можно прийти к идее реализации комплекса следующих функций в соответствии с конкретными задачами исследования безопасности:

- анализ конфигурации сети;
- анализ процессов, происходящих в сети;
- моделирование действий злоумышленников на основе данных о сети;
- построение цепочки возможных атакующих действий, выполняемых из различных точек сети и направленных на реализацию различных угроз безопасности;

• определение уязвимостей и узких мест в защите (наиболее критических компонентов компьютерной сети);

• вычисление различных показателей защищенности и определение общего уровня защищенности;

• сопоставление полученных показателей с требованиями заказчика и выработка рекомендаций по усилению защищенности информационной системы.

Выводы

Построение современной безопасной Wi-Fi сети — это сложная задача, решить которую по силам только специализирующимся в этой области компаниям. Оценить уровень безопасности сети, построенной некоторое время назад, порой еще сложнее, поскольку за время ее существования в базовую конфигурацию сети могли быть внесены недокументированные изменения, и их влияние на общую безопасность сети на момент модернизации не выяснено. Руководство компаний, в чьем ведении находятся беспроводные Wi-Fi сети, должно объективно оценивать риски, связанные с небезопасным использованием корпоративной информации.

Наиболее перспективным подходом для решения задачи аудита безопасности беспроводной Wi-Fi сети представляется использование комплексного автоматизированного подхода с применением сертифицированного программного средства анализа защищенности беспроводных сетей, которое позволит исследовать беспроводную сеть на уязвимость, провести аудит паролей, настроек и версий программного обеспечения оборудования.

ЛИТЕРАТУРА

1. **Белорусов Д.И., Корешков М.С.** WIFI-сети и угрозы информационной безопасности // Специальная техника. 2009. № 6. С. 2–6.
2. **Борисов В.И., Щербаков В.Б., Ермаков С.А.** Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11 // Информация и безопасность. 2008. Т. 11. № 3. С. 431–434.
3. **Владимиров А.А., Гавриленко К.В., Михайловский А.А.** Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей. М.: НТ Пресс, 2005. 464 с.
4. **Гепко И.А., Олейник В.Ф., Чайка Ю.Д., Бондаренко А.В.** Современные беспроводные сети. Состояние и перспективы развития. Киев: ЕКМО, 2009. 672 с.
5. **Гордейчик С.В., Дубровин В.В.** Безопасность беспроводных сетей. М.: Горячая линия-Телеком, 2008. 288 с.
6. **Дорофеев А.В.** Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. INSIDE, 2010. № 6. С. 72–73.
7. **Зегжда Д.П., Коваленко С.Л.** Проблемы безопасности беспроводных сетей семейства IEEE 802.11a/b/g // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 45–49.
8. **Иващук И.Ю.** Модель и метод построения семейства профилей защиты для беспроводной сети. СПб.: Изд. СПбГУИТМО. 133 с.
9. **Львович Я.Е., Фефилов И.И., Савинский П.Л., Кащенко Г.А.** Выбор технологии построения защищенных сетей беспроводной связи // Информация и безопасность. 2009. Т. 12. № 2. С. 263–268.
10. **Марков А.С., Фадин А.А., Цирлов В.Л.** Средства и технологии анализа защищенности // Информатизация и информационная безопасность правоохранительных органов. М.: Академия управления МВД России, 2011. С. 434–437.
11. **Мерритт М., Поллино Д.** Безопасность беспроводных сетей. М.: ДМК Пресс, 2004. 288 с.
12. **Пролетарский А.В., Баскаков И.В., Чирков Д.Н.** Беспроводные сети Wi-Fi. М.: БИНОМ, 2007. 178 с.