МЕТОДЫ ЗАЩИТЫ И АТАКИ НА БЕСПРОВОДНЫЕ СЕТИ

Карнаух Максим Михайлович

Гродненский государственный университет им.Янки Купалы,
факультет математики и информатики,
кафедра системного программирования и компьютерной безопасности
студенты 3 курса специальности «Компьютерная безопасность»

Научный руководитель: Ващило Владимир Витольдович, ст.пр., магистр

В работе описываются краткие сведения о беспроводных сетях, в частности – Wi-Fi, так как эта сеть встречается даже в удаленных уголках мира и означает для многих беспроводной доступ в интернет с помощью смартфона или ноутбука. Будут проанализированы методы шифрования WEP, WPA, WPA и рассмотрены найденные уязвимости в них. В частности будет рассмотрены практические действия в операционной системе Kali Linux для проведения тестирования безопасности своей сети, а так же будут даны рекомендации для обеспечения безопасности своей сети Wi-Fi.

Ключевые слова: МЕТОДЫ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ, ВИДЫ ПОДКЛЮЧЕНИЙ, БЕЗОПАСНОСТЬ ПОДКЛЮЧЕНИЯ, УЯЗВИМОСТИ, АТАКИ, WI-FI

В наше время бурно развиваются беспроводные технологии в области информатизации, так как не всегда удобен, а иногда даже не возможен монтаж проводных линий связи. С каждым днём технологии движутся вперёд, следовательно, появляются новые уязвимости и атаки.

Термин «уязвимость» в информационной безопасности используется для обозначения недостатка в той или иной системе, используя которую можно намеренно нарушать её целостность и вызывать некорректную работу. Атаки на беспроводные сети могут быть произведены при нахождении атакующего в зоне покрытия сети, однако ему предоставляется больше возможностей по сравнению с атаками через сеть интернет удаленно.

Для предотвращения угроз похищения пользовательских и корпоративных данных или приведения беспроводного устройства к отказу в обслуживания при передаче по беспроводной сети существуют определённые методы их защиты. Каждый из этих методов нацелен на обеспечение защиты от определённого круга атак. Однако, даже с учётом использования таких средств защиты существует вероятность взлома и кражи пользовательских данных при использовании хакером социальной инженерии.

Классификация и области применения беспроводных сетей

Беспроводные сети можно разделить на 4 группы по дальности действия:

1. WPAN — Беспроводные персональные сети. К примеру этой технологии можно отнести Bluetooth, ZigBee, 6loWPAN.
2. WLAN — Беспроводные локальные сети. К примеру этой технологии можно отнести Wi-Fi.
3. WMAN — Беспроводные сети городского масштаба. Пример данной технологии является WiMAX.

4. WWAN — Беспроводные глобальные сети. К ним относятся технологии GPRS, UMTS, LTE, EDGE, EV-DO, HSPA.

По топологии сети определяются как: «Точка-точка»[1].и «Точка-многоточка».
По области применения беспроводные сети являются: Корпоративными и Операторскими

Типы шифрования и их уязвимости

WEP появился в 1997 году. Джесси Уолкер в 2000 году опубликовал статью, которая описывает уязвимости алгоритма WEP, а именно слабые места: малой разрядности ключа и вектора инициализации, в механизмах передачи ключей и проверки целостности данных, способах аутентификации[2]. WEP существует в двух вариантах: WEP-40 и WEP-104. Отличаются друг от друга всего лишь длинной ключа. С 2004 года такой тип шифрования для беспроводной сети использовать не рекомендуется, т.к. он подвержен многим атакам, такие как: атака Фларера-Мантина-Шамира, атака KoreK, атака Тевса-Вайнмана-Пышкина.

WPA появился в 2004 году, вслед за уязвимым WEP алгоритмом, и имеет ряд преимуществ, например более стойкий криптографический алгоритм. WPA шифрование состоит из ряда технологий: 802.1X, EAP, TKIP, MIC[3]. Технология WPA предназначена для использования с сервером проверки подлинности 802.1X, который распределяет различные ключи каждому пользователю. Однако ее также можно использовать в менее безопасном режиме Pre-Shared Key (PSK).

WPA первой версии использует протокол шифрования TKIP, который уже давно устарел. Протокол TKIP в наше время уже не считается безопасным так как имеет «дыры». Например, не защищает от атаки полного перебора. Время подбора пароля представлено в таблице 2.1, при скорости 10 млн. паролей в секунду.

Таблица 2.1 — Время подбора пароля

Алфавит	6 символов	8 символов	10 символов	12 символов
26 (латиница один регистр)	31 сек	5 ч 50 мин	163 дня	303 года
52 (латиница с переменным регистром)	33 мин	62 дня	458 лет	1239463 года
62 (латиница разного регистра плюс цифры)	95 мин	252 дня 17 ч	2661 год	10230425 лет
68 (литиница разного регистра плюс цифры и знаки , . ! ?)	2 ч 45 мин	529 дней	6703 года	30995621 лет
80 (латиница разного регистра плюс любые спец символы)	7 ч 30 мин	5 лет 4 месяца	34048 лет	217908031 год

Однако, если пароль состоит из 8-ми цифр (самое популярное это дата рождения в формате ddmmyyyy, номера телефонов и др.), то его можно легко перебрать. Но время перебора зависит не только от сложности пароля, а еще от: типа процессора (CPU либо GPU), их тактовой частоты и многопоточности. Эта атака распространяется только на PSK режим.

В целях изучения атаки полным перебором было решено провести атаку на лабораторном компьютере. Для этого понадобились: компьютер, утилита hashcat, файл с «хендшейком» конкретной Wi-Fi сети с роутером.

Характеристики вычислительной машины:

- Процессор Intel® Core™ i5-5200U, 2,2 ГГц 4 ядра
- Видеокарта AMD Radeon R9 M375, 1015 МГц, 2 ГБ
- Оперативная память 8 ГБ

Средняя скорость перебора на CPU — 3597 паролей в секунду(Рисунок 2.3).

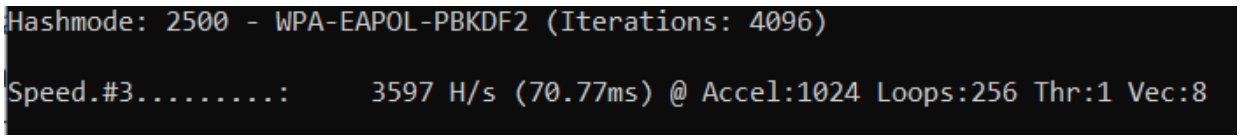

Рисунок 2.3 – Скорость полного перебора на графическом процессоре

Средняя скорость перебора на GPU — 33915 паролей в секунду (Рисунок 2.4).

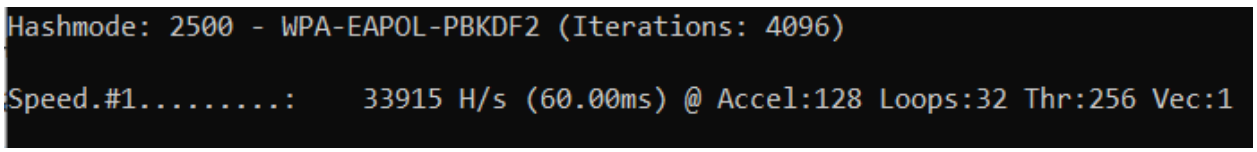

Рисунок 2.4 – Скорость полного перебора на центральном процессоре

Видно, что скорость перебора на графическом процессоре практически в 10 раз больше чем на центральном процессоре.

Минимальная длина пароля– 8 символов. Допустим у пользователя стоит пароль 8 символов, и это дата его рождения. Допустим пароль имеет значение 31122000. Учитывая производительность вычислительной машины он будет подобран на CPU за 2ч 25 минуты, на GPU за 16 минут.

В стандарте шифрования WPA 2 разработчики реализовали CCMP и применили технологию шифрования AES [4]. WPA 2 благодаря этим технологиям стал более защищённым, чем предыдущий протокол.

AES шифрование не сравнимо с TKIP, так как использует более защищенный алгоритм шифрования. Алгоритм включает в себя 128, 192 или 256-битный блоковый шифр, не подверженный уязвимостям TKIP. В теории взломать AES даже с 128 битным блочным шифром займёт более сотни при использовании средней вычислительной мощности обычного компьютера. Однако, атака подбора пароля применима к этому протоколу и действует аналогично с протоколом первой версии.

Уязвимости WPS

По протоколу WPS есть 3 способа подключения:

1. При помощи пин-кода, который отображен на роутере. Его следует ввести в устройство при подключении к сети.

2. При нажатии на кнопку WPS на точке доступа. После нажатия нужно подключиться к сети в течении интервала времени (обычно 2 минуты).

3. WPS режим всегда включен и подключиться можно без манипуляций с роутером.

Много маршрутизаторов предоставляемых провайдером в Республике Беларусь работают по 3 принципу. Для подключения нужен 8-мизначный числовой пин-код, но так как в протоколе WPS есть ошибка безопасности, то достаточно угадать лишь 4 цифры из первой половины ключа, и 3 цифры после подобранных первых четырех. Последняя цифра генерируется атакующим по известной формуле. Следовательно существует10000 + 1000 = 11000 вариантов ключей.

В секунду можно посылать от 10 до 50 запросов по протоколу WPS, а время взлома составит от 3 до 15 часов в среднем. Если производителем роутера будет задано ограничение попыток входа по времени, то даже если посылать 1 запрос в минуту, то понадобиться не более 7 дней в среднем.

Попробуем на примере рассмотреть данную уязвимость.

Для этого потребуются утилиты: Reaver, Wash на Kali Linux и беспроводной адаптер Wi-Fi, лабораторная ТД[5].

Вводим команду **wash –i wlan1** и ждем получение информации о найденных сетях. Обращаем внимание на колонку WPS Locked и видим, что везде стоит No, а это значит, что WPS включен и можно производить атаку (Рисунок 3.8).

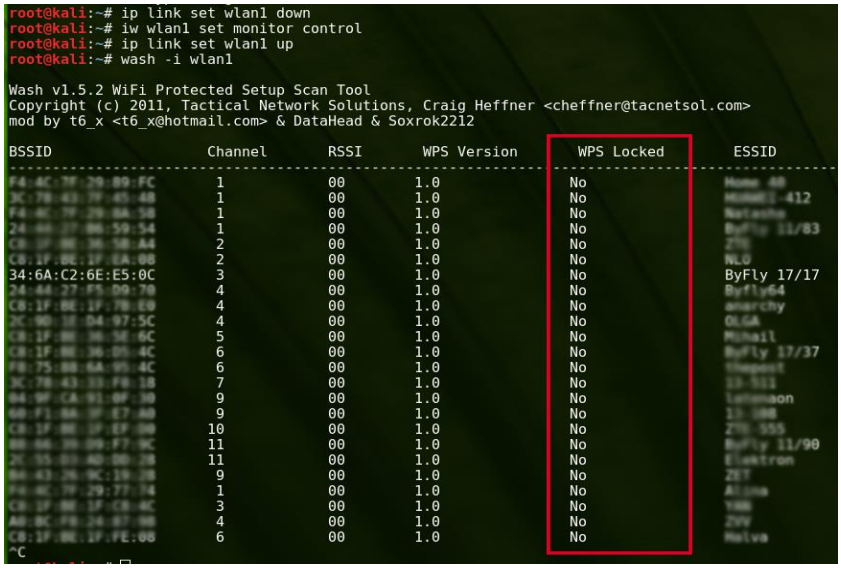

Рисунок 3.8 – Скриншот программы wash

Далее пишем команду **reaver -b 34:6A:C2:6E:E5:0C -i wlan1 –vvv**

Начинается перебор ключей по алгоритму. Так же можем видеть модель роутера, в данном случае это Huawei HG824H-256M. Такие же маршрутизаторы используются по всему дому, так как провайдер в доме проложил оптоволокно и заключил новые договора со всеми жильцами на получение нового оборудования.

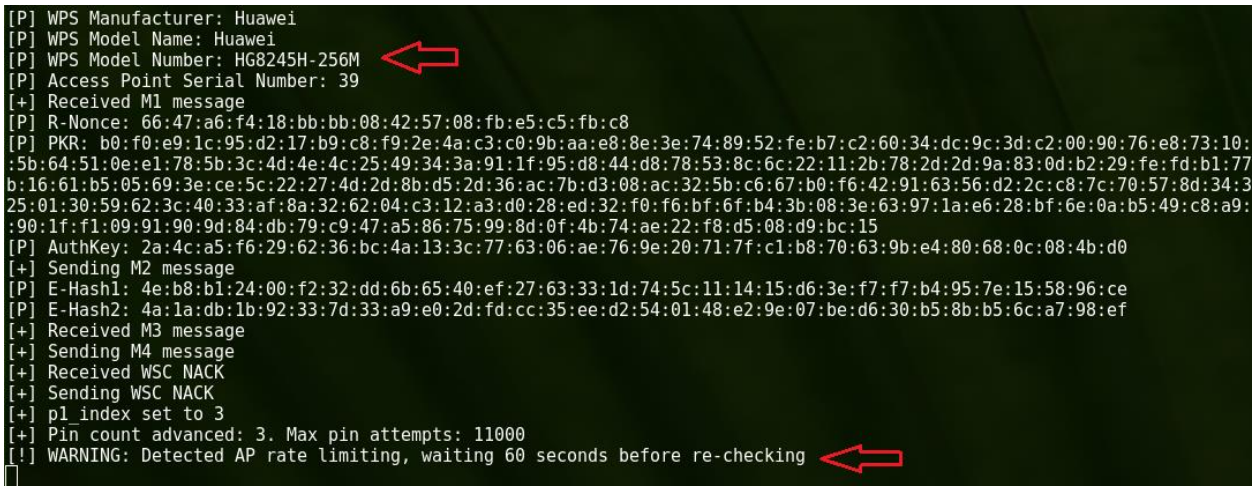

Рисунок 3.9 – Скриншот программы Reaver

Через несколько итераций маршрутизатор замечает частые попытки подключения по WPS и ограничивает доступ на 60 секунд. Это позволяет увеличить время полного перебора до 7 дней как упоминалось ранее.

Рекомендации по повышению безопасности использования Wi-Fi

По статистике более 70% владельцев гаджетов часто пользуются общедоступными ТД Wi-Fi, тем самым подвергая себя риску раскрытия личной информации и цифровых идентификационных данных. Причем, если гаджет на защищен надежным антивирусом и имеет устаревшее ПО, то вероятность хищения данных только увеличивается.

По возможности нужно стараться избегать подключений к открытым и общедоступным сетям, а если это необходимо, то использовать подключение через VPN.

Для обеспечения безопасности домашней беспроводной сети следует:

1. Использовать самую свежую прошивку для маршрутизатора.
2. Пользоваться маршрутизатором именитых брендов, прошедших сертификацию Wi-Fi альянсом.
3. При наличии функции WPS отключить её в настройках роутера.
4. Применять технологию WPA 2 с шифрованием AES.
5. Скрыть SSID точки доступа.
6. Установить сложный пароль, включающий в себя более 12 символов, используя специальные символы, буквы верхнего и нижнего регистра.
7. Ограничить доступ всем посторонним устройствам при подключении. Настроить White List в настройках роутера с MAC адресами доверенных устройств.

При возникновении подозрения в легальности ТД необходимо сразу разорвать соединение и не использовать её. Так как при использовании фишинговой сети хакерам не составит большого труда похищение конфиденциальных данных.

Заключение

В ходе исследования было проведено изучение существующих методов защиты, углубленно была изучена технология Wi-Fi. Было выполнено описание одной из самых популярных атак на беспроводные сети, а так же были определены способы их предотвращения. Удалось выявить недостатки протокола WPS

Данное исследование может применяться при создании локальной домашней беспроводной сети, а так же для создания корпоративной сети, где необходима конфиденциальность и целостность передаваемых данных. Данное исследование может также осведомить широкий круг общественности об описанных в этом исследовании

атаках и мер защиты для обеспечения конфиденциальности данных при подключении к общественным сетям.

Литература

1. Беделл, П. Сети. Беспроводные технологии / Беделл П. – Москва: НТ пресс, 2008. – 58 с.
2. Jesse R. Walker. Unsafe at any key size. An analysis of the WEP encapsulation / Jesse R. Walker – Орегон, 2000. – 2 с.
3. WPA [Электронный ресурс] / Wikipedia: бесплатная энциклопедия в сети интернет. – Wikipedia, 2015. – Режим доступа: https://ru.wikipedia.org/wiki/WPA – Дата доступа: 03.12.2019.
4. Баричев С. Г., Гончаров В. В., Серов Р. Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — С. 30–35. — 176 с.
5. Ализар А. Получаем WPA ключ для Wi-Fi с помощью уязвимой технологии WPS/ А. Ализар // Хакер [Электронный ресурс]. – 2012. Режим доступа: https://xakep.ru/2012/11/08/wifi-key-with-wps/. – Дата доступа: 30.11.2019.