Scientific and Practical Cyber Security Journal (SPCSJ) 3(1): 1-5 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

АЛГОРИТМЫ БЕЗОПАСНОСТИ WI-FI – ИХ ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

WI-FI SECURITY ALGORITHMS – THEIR STRENGTHS AND WEAKNESSES

B.Horbatenko V.Stopin, V.Ivanov
Kharkiv National University of Radio Electronics (NURE), «Computer science» faculty, department of «System engineering»

ABSTRACT. The article describes the new Wi-Fi security algorithm – WPA3. The advantages of this technology and its innovations are proposed. For comparison, outdated protection methods – WEP, WPA, WPA2 are analyzed and described. In the article it is shown the principle, vulnerabilities and shortcomings of their work.

АННОТАЦИЯ. В статье описан новый алгоритм безопасности Wi-Fi - WPA3. Предлагаются преимущества этой технологии и её нововведения. Для сравнения проанализированы и описаны устаревшие методы защиты - WEP, WPA, WPA2. В статье продемонстрированы принципы, уязвимости и недостатки их работы.

KEYWORDS: Wi-Fi, WEP, WPA, WPA2, WPA3, Security.

На сегодняшний день каждый знает, что значит слово «Wi-Fi». Без него сложно представить повседневную жизнь. Миллиарды людей во всем мире зависят от Wi-Fi, используют его для совершения покупок, просмотра роликов в Интернет, взаимодействуют с ним в «умных» домах, банках и в конце концов в общении друг с другом через мессенджеры и социальные сети. Число используемых точек Wi-Fi с каждым днем растет и вопрос их безопасности является крайне важным элементом защиты персональных данных.

Первые в истории Wi-Fi точки были доступными для всех, никаких алгоритмов безопасности и защищённых каналов не было. Однако спустя некоторое время, остро возник вопрос безопасности, так как находились злоумышленники, которые злоупотребляли незащищенностью и всячески вредили публичным сетям. Таким образом появился первый алгоритм для обеспечения безопасности сетей Wi-Fi – WEP (Wired Equivalent Privacy). Для шифрования данных в WEP используется ключевой поток, который образуется при смешивании пароля и вектора инициализации (рисунок 1).

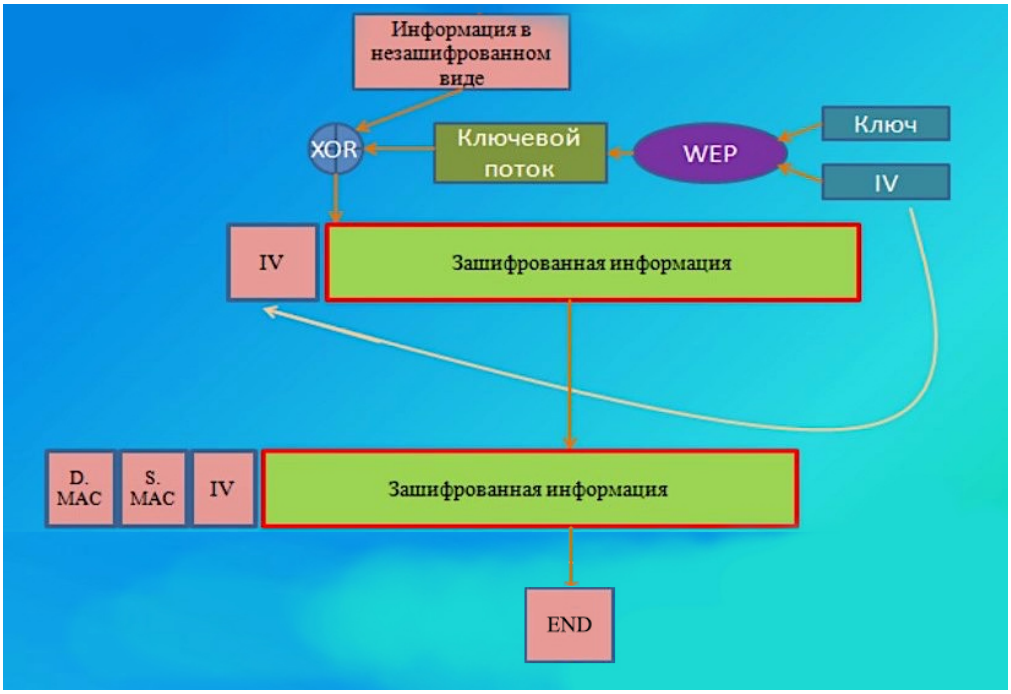

Рисунок 1 – Алгоритм работы WEP

Вектор инициализации в WEP — это постоянно меняющееся 24-битное число и можно было бы предположить, что взломать или подобрать его невозможно, однако с увеличением вычислительных мощностей персональных компьютеров длина вектора инициализации стала недостаточной. Методом подбора можно подобрать необходимые значения кадров, для которых вектор инициализации будет одинаковым. Таким образом взлом данного алгоритма стал сводится к нескольким минутам.

Решением этой проблемы было разработка нового алгоритма безопасности – WPA. WPA являлся модификацией WEP, новшеством которой было внедрение WPS – стандарта, который упрощал подключение к беспроводной сети. Для обеспечения целостности сообщений он использовал протокол целостности TKIP или Temporal Key Integrity, в то время, как WEP использовал CRC или Cyclic Redundancy Check. Считалось, что TKIP намного сильнее, чем CRC. Однако TKIP стала объектом хакеров и в ней были найдены уязвимости, которые позволяли эксплуатировать её и перехватывать сообщения в сети. Для исправления этой уязвимости было внедрено решение обрывать все подключения на 60 секунд при попытках подбора ключей. Хакеры воспользовались данным решением и посылали фиктивные пакеты, которые позволяли выводить сеть из строя. Далее были найдены и иные уязвимости, которые позволяли иметь полный контроль над сетью. Таким образом WPA себя продемонстрировала не с лучшей стороны. Это привело к тому, что возникла необходимость искать новый алгоритм безопасности.

В 2004 году был запущен новый алгоритм на устройствах, точнее модификация его предшественника – WPA2. Сильной стороной оказалось индивидуальное шифрование данных каждого пользователя, а алгоритмом шифрования стал AES, что значительно повысило уровень безопасности. Долгое время WPA2 считался безопасным, однако в 2017 году была опубликована уязвимость, которая позволяет взламывать Wi-Fi точки даже с алгоритмом WPA2.

Уязвимость эта имеет название KRACK (Key Reinstallation Attack) – атака с

переустановкой ключа [1]. При атаке с переустановкой ключа злоумышленник заставляет жертву переустанавливать уже используемый ключ. Это достигается путем манипулирования и воспроизведения криптографических сообщений рукопожатия. Когда жертва переустанавливает ключ, связанные параметры, такие как номер инкрементного передаваемого пакета и номер принимаемого пакета, сбрасываются до их начального значения. Когда клиент присоединяется к сети, он выполняет четырехстороннее рукопожатие для согласования нового ключа шифрования (рисунок 2). Установка этого ключа произойдет тогда, когда будет получено 3 сообщение о четырехстороннем рукопожатии. После того как ключ установлен, он будет использоваться для шифрования обычных кадров данных с использованием протокола шифрования. Однако, поскольку сообщения могут быть потеряны или отброшены, точка доступа будет повторно передавать сообщение 3, если оно не получило соответствующий ответ в качестве подтверждения. В результате клиент может получить сообщение 3 несколько раз. Каждый раз, когда он получает это сообщение, он переустанавливает один и тот же ключ шифрования и, таким образом, сбрасывает инкрементный номер передаваемого пакета и получает номер принимаемого пакета, используемый протоколом шифрования. Злоумышленник может принудительно выполнить эти одноразовые сбросы путем сбора и воспроизведения повторных передач сообщения 3 четырехстороннего рукопожатия. Таким образом злоумышленник может подделать пакеты, дешифровать и воспользоваться ими. Атака работает против всех современных защищенных сетей Wi-Fi. Некоторые компании выпустили обновления, позволяющие уменьшить возможности этой уязвимости, однако не все пользователи обновляют свои роутеры, что может вести лишь к усугублению ситуации с безопасностью.

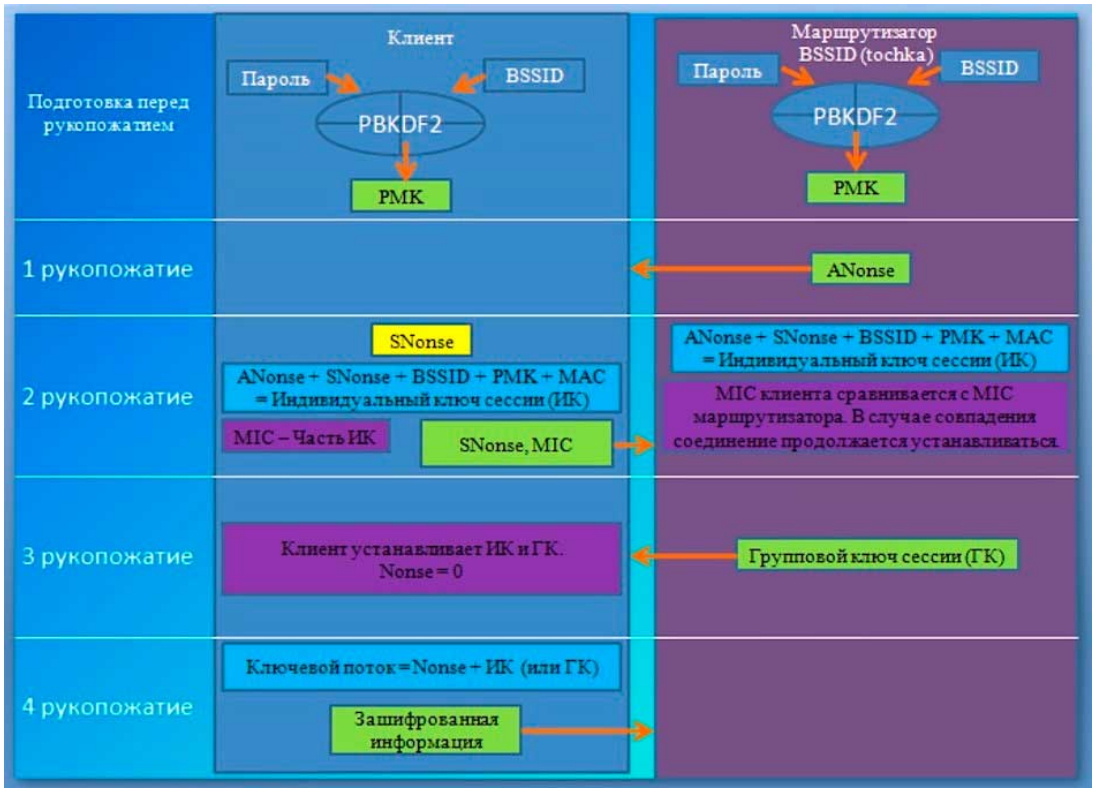

Рисунок 2 – Четырехстороннее рукопожатие алгоритма WPA2

На рисунке 3 представлена статистика – общее количество Wi-Fi точек на планете и алгоритмы безопасности, используемые на них [2].

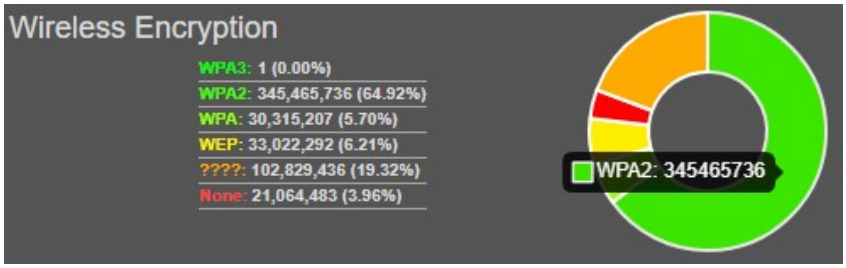

Рисунок 3 – Алгоритмы шифрования Wi-Fi

Как видно на рисунке 2, почти 65% точек доступа используют алгоритм WPA2, 19.32% используют неизвестные методы шифрования и защиты, 5.70% используют WPA, 6.21% используют WEP, невзирая на его небезопасность в целом, и 3.96% не используют методы защиты Wi-Fi вообще.

Рассмотрим какую опасность в себе несет получение злоумышленником доступа к Wi-Fi точке. Предположим, что злоумышленник получил доступ к точке, которой пользуются корпоративные сотрудники одной из крупных компаний. Злоумышленник может совершить перехват сообщений, которые сотрудники отправляют в мессенджерах и в последствии использовать данную информацию против этого сотрудника или целой компании. Помимо этого, есть возможность кражи паролей и кукис файлов браузера. Если пользователь использует корпоративную почту, то злоумышленник может заполучить доступ к письмам на почте. При наличии доступа к точке доступа Wi-Fi можно подменить файлы, которые пользователь качает в сети, тем самым подменив их на вредоносный код. Множество случаев со взломами были связаны именно с запуском вредоносных программ, которые приводили к крупным ущербам, как финансовым, так и вреду репутации компании. Поэтому вопрос безопасности точек доступа Wi-Fi в коммерческих структурах должен быть основополагающим. Для этого и разрабатываются новые алгоритмы безопасности, дабы предотвращать вероятность взломов со стороны злоумышленников.

В связи с нахождением уязвимости в WPA2 была начата разработка нового алгоритма безопасности, который получил название – WPA3. Он является новым поколением систем безопасности Wi-Fi и еще не находится в массовом доступе на рынке (на момент написания статьи насчитывалось всего 10 моделей, которые поддерживают WPA3). WPA3 добавляет новые функции, упрощающие безопасность Wi-Fi, обеспечивающие более надежную аутентификацию, повышающие криптографическую стойкость для рынков высокочувствительных данных и поддерживающие устойчивость критически важных сетей [3]. Таким образом, в WPA3 была внедрена защита от перебора по словарю или метода «грубой силы», после нескольких неудачных попыток происходит блокировка, происходит это благодарю методу SAE [4]. SAE (Simultaneous Authentication of Equals) – новый метод аутентификации устройства, пытающегося подключиться к сети, это вариант «установления связи по методу стрекозы», использующего криптографию для предотвращения угадывания пароля злоумышленником. Поддержка прямой секретности позволяет сохранить конфиденциальность данных даже при успешном взломе злоумышленником. Совершенная прямая секретность (PFS) означает, что сеансовый ключ, генерируемый с использованием долговременных ключей, не будет скомпрометирован, если один или несколько из этих долговременных ключей будут скомпрометированы в будущем.

В открытых сетях, трафик индивидуального устройства так же будет шифроваться при помощи протокола Enhanced Open (чего нет в данный момент в WPA2). Enhanced Open

использует оппортунистическое беспроводное шифрование (Opportunistic Wireless Encryption, OWE), чтобы защищаться от пассивного подслушивания [5]. Для OWE не требуется дополнительная защита с аутентификацией – оно концентрируется на улучшении шифрования данных, передаваемых по публичным сетям, с целью предотвратить их кражу. Оно также предотвращает «простую инъекцию пакетов», в которой атакующий пытается нарушить работу сети, создавая и передавая особые пакеты данных, выглядящие, как часть нормальной работы сети. На сегодняшний день Wi-Fi работает с безопасностью в 128 бит. WPA3 внедряет новые 192 и 256 битные протоколы безопасности, которые позволят обеспечивать более эффективную защиту данных.

Однако не все так радужно, как описано выше. WPA3 поддерживает обратную совместимость с алгоритмом WPA2, что несомненно может вести к негативным последствиям. Внедрение SAE хоть и ведет к усложнению процесса перебора паролей, однако полностью его не исключает. Помимо этого, стоит предположить, что если злоумышленник все-таки получает доступ к точке доступа Wi-Fi (либо разворачивают свою собственную точку доступа), то он все так же сможет перехватывать траффик.

Разработчики роутеров однозначно воспользуются выходом нового алгоритма безопасности, для увеличения продаж своих устройств. Не исключено, что поддержка старых моделей устройств производители целенаправленно обновлять не будут, дабы пользователи приобретали новые. Будем надеяться, что WPA3 продемонстрирует себя с лучшей стороны в плане безопасности, нежели его предшественники.

REFERENCES

1. https://www.krackattacks.com
2. https://wigle.net/stats
3. https://www.wi-fi.org/discover-wi-fi
4. https://ieeexplore.ieee.org/document/7786995
5. https://tools.ietf.org/html/rfc8110