УДК 004.056.5

Субботин Егор Сергеевич,
Донской государственный технический университет
Subbotin Egor Sergeyevich, student,
Don State Technical University

Чухлатов Максим Сергеевич, студент,
Донской государственный технический университет
Chukhlatov Maxim Sergeyevich, student,
Don State Technical University

Шевчук Петр Сергеевич,
доктор технических наук, профессор,
профессор кафедры «Информационная безопасность
в вычислительных системах и сетях»,
Донской государственный технический университет
Shevchuk Petr Sergeyevich,
Doctor of Technical Sciences, Professor,
Professor, Department of Information Security
in Computing Systems and Networks,
Don State Technical University

УЯЗВИМОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ В СЕТЯХ WI-FI (WPA2/WPA3) И МЕТОДЫ ИХ УСТРАНЕНИЯ
AUTHENTICATION PROTOCOL VULNERABILITIES IN WI-FI NETWORKS (WPA2/WPA3) AND METHODS FOR THEIR MITIGATION

Аннотация. В работе рассмотрены уязвимости протоколов аутентификации сетей Wi-Fi семейств WPA2 и WPA3. Проанализированы атаки на четырёхстороннее рукопожатие WPA2 (перехват с последующим офлайн-перебором, PMKID-атака, переустановка ключа KRACK) и на рукопожатие SAE в WPA3 (атаки по побочным каналам Dragonblood и понижение версии в переходном режиме). Приведена сравнительная оценка стойкости и предложены методы устранения выявленных уязвимостей: переход на WPA3-SAE, обновление программного обеспечения, преобразование Hash-to-Element, обязательная защита управляющих кадров и отказ от переходного режима.

Abstract. The paper examines the authentication protocol vulnerabilities of the WPA2 and WPA3 Wi-Fi families. Attacks on the WPA2 four-way handshake (capture with subsequent offline brute force, the PMKID attack, the KRACK key reinstallation) and on the WPA3 SAE handshake (the Dragonblood side-channel attacks and version downgrade in transition mode) are analysed. A comparative resistance assessment is given, and mitigation methods are proposed: migration to WPA3-SAE, software updates, the Hash-to-Element transform, mandatory protected management frames and abandonment of transition mode.

Ключевые слова: WPA2; WPA3; SAE; четырёхстороннее рукопожатие; KRACK; Dragonblood.

Keywords: WPA2; WPA3; SAE; four-way handshake; KRACK; Dragonblood.

Введение.

Беспроводные сети стандарта IEEE 802.11 (Wi-Fi) получили повсеместное распространение, что делает защиту доступа к ним одной из значимых задач информационной

безопасности телекоммуникационных систем. Ключевую роль в защите играет протокол аутентификации, устанавливающий подлинность сторон и вырабатывающий сеансовые ключи. Эволюция механизмов защиты прошла путь от заведомо небезопасного WEP к WPA2 на основе стандарта IEEE 802.11i и далее к WPA3, представленному Wi-Fi Alliance в 2018 году. Несмотря на совершенствование протоколов, в них последовательно выявляются уязвимости: для WPA2 – атака переустановки ключа KRACK (2017), для WPA3 – комплекс атак Dragonblood (2019).

Цель работы – проанализировать уязвимости протоколов аутентификации WPA2 и WPA3, дать сравнительную оценку их стойкости и систематизировать методы устранения выявленных недостатков.

Механизмы аутентификации в WPA2 и WPA3.

В режиме WPA2-Personal аутентификация основана на общем секрете (Pre-Shared Key, PSK). Из парольной фразы и идентификатора сети SSID вырабатывается парный мастер-ключ:

$$PMK = PBKDF2(PSK, SSID, 4096, 256) \quad (1)$$

На основе PMK в ходе четырёхстороннего рукопожатия (four-way handshake) стороны обмениваются случайными значениями (ANonce, SNonce) и вырабатывают парный временный ключ PTK, используемый для шифрования трафика. Схема рукопожатия приведена на рисунке 1. В режиме WPA3-Personal вместо этого применяется рукопожатие SAE (Simultaneous Authentication of Equals, известное также как Dragonfly) – протокол с аутентификацией по паролю (PAKE), обеспечивающий прямую секретность и стойкость к офлайн-перебору. Дополнительно WPA3 делает обязательной защиту управляющих кадров (Protected Management Frames, PMF, стандарт 802.11w).

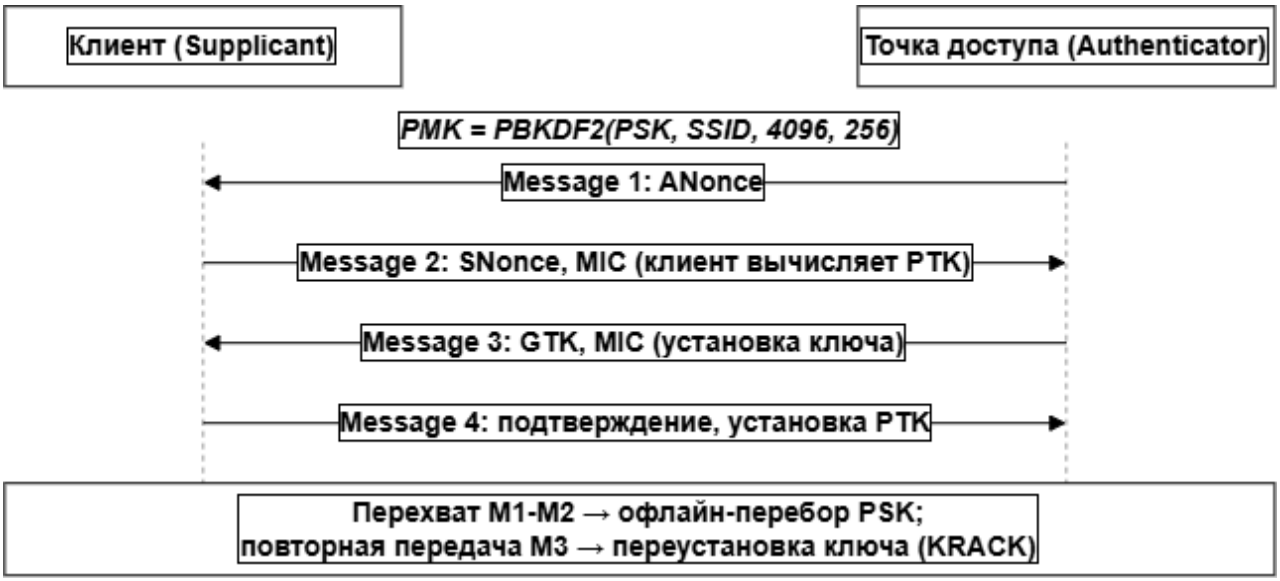

Рисунок 1. Четырёхстороннее рукопожатие WPA2 и точки воздействия атак

Уязвимости WPA2.

Основная слабость WPA2-Personal связана с возможностью офлайн-перебора парольной фразы. Перехватив сообщения рукопожатия, нарушитель может в автономном режиме проверять кандидаты пароля, вычисляя PMK и сверяя имитовставку (MIC). Ожидаемое время такого перебора определяется размером пространства паролей и производительностью атакующей системы:

$$T_{cp} = \frac{|A|^L}{2R} \quad (2)$$

где |A| – мощность используемого алфавита, L – длина пароля, R – число проверяемых вариантов в секунду. Из выражения (2) видно, что стойкость к перебору критически зависит от длины и сложности парольной фразы. Разновидностью данной угрозы является PMKID-атака, позволяющая получить необходимые для перебора данные из одного кадра, передаваемого точкой доступа, без участия легитимного клиента.

Отдельный класс представляет атака переустановки ключа KRACK (Key Reinstallation Attack), обнаруженная в 2017 году. Нарушитель, воздействуя на третье сообщение рукопожатия, вынуждает клиента повторно установить уже используемый ключ, что приводит к сбросу счётчиков и повторному использованию последовательности шифрования. Это позволяет расшифровывать, а в ряде конфигураций и подделывать передаваемые кадры. Уязвимость затрагивала практически все реализации WPA2 и была устранена обновлениями программного обеспечения клиентов и точек доступа.

Уязвимости WPA3.

Протокол WPA3, несмотря на принципиально более стойкое рукопожатие SAE, также оказался подвержен ряду атак, объединённых названием Dragonblood и опубликованных в 2019 году. Первую группу составляют атаки по побочным каналам (side-channel): анализируя время выполнения или обращения к кэшу при кодировании пароля в точку эллиптической кривой (процедура hunting-and-pecking), нарушитель постепенно сокращает пространство возможных паролей (так называемые атаки разделения пароля). Вторую группу образуют атаки понижения. В переходном режиме (WPA3-Transition), обеспечивающем совместимость с устаревшими клиентами, нарушитель может развернуть поддельную точку доступа, поддерживающую только WPA2, и вынудить клиента установить соединение по WPA2 с последующим словарным перебором. Кроме того, согласование криптографической группы в SAE не защищено криптографически, что делает возможной атаку группового понижения. Наконец, продемонстрирована возможность отказа в обслуживании за счёт перегрузки точки доступа вычислительно затратными защитными операциями SAE.

Методы устранения.

Устранение рассмотренных уязвимостей достигается сочетанием протокольных и организационно-технических мер. Радикальным средством против офлайн-перебора служит переход на рукопожатие SAE: поскольку каждая проверка пароля требует отдельного интерактивного обмена с точкой доступа, автономное ускорение перебора становится невозможным, а его стоимость определяется выражением:

$$T_{SAE} = \frac{|A|^L}{2} \cdot t_h \qquad (3)$$

где th – время одного интерактивного рукопожатия. В отличие от выражения (2), здесь перебор является онлайновым, поддаётся ограничению скорости и обнаружению. Атаки Dragonblood по побочным каналам устраняются заменой процедуры hunting-and-pecking на преобразование Hash-to-Element (H2E), выполняемое за постоянное время и не зависящее от значения пароля. Против атак переустановки ключа KRACK применяется своевременное обновление программного обеспечения. Атаки понижения версии нейтрализуются отказом от переходного режима (использование режима WPA3-only) и запоминанием клиентом факта поддержки сетью WPA3-SAE. Обязательная защита управляющих кадров (PMF) исключает подделку и перехват служебных сообщений. Для корпоративных сетей предпочтительно применение аутентификации 802.1X/EAP-TLS с индивидуальными учётными данными вместо общего пароля.

Сопоставление механизмов аутентификации WPA2 и WPA3 приведено в таблице 1, а соответствие выявленных уязвимостей методам их устранения – на рисунке 2.

Таблица 1

Сравнение механизмов аутентификации WPA2 и WPA3

Показатель	**WPA2-Personal**	**WPA3-Personal**
Протокол аутентификации	4-стороннее рукопожатие (PSK)	SAE (Dragonfly, PAKE)
Стойкость к офлайн-перебору	низкая (перехват рукопожатия)	высокая (перебор только онлайн)
Прямая секретность (PFS)	отсутствует	обеспечивается
Защита управляющих кадров (PMF)	опциональна	обязательна
Известные атаки	KRACK, PMKID, словарные	Dragonblood (побочные каналы, понижение)
Основные меры устранения	патчи ПО, стойкий пароль	H2E, режим WPA3-only, патчи

Рисунок 2. Соответствие уязвимостей методам их устранения

Заключение.

В работе систематизированы уязвимости протоколов аутентификации Wi-Fi семейств WPA2 и WPA3 и методы их устранения. Показано, что основная слабость WPA2 – подверженность офлайн-перебору при перехвате рукопожатия, а также атаки PMKID и KRACK, тогда как WPA3, устраняя офлайн-перебор за счёт рукопожатия SAE, приобретает новые классы уязвимостей, связанные с побочными каналами и понижением версии в переходном режиме. Установлено, что комплексное применение мер – переход на WPA3-SAE с преобразованием Hash-to-Element, обновление программного обеспечения, обязательная защита управляющих кадров и отказ от переходного режима – обеспечивает существенное повышение защищённости беспроводного доступа. Полученные результаты могут быть использованы при проектировании и аудите защищённых беспроводных сегментов телекоммуникационных систем.

Список литературы:

1. Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 // Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS). – 2017. – P. 1313-1328.
2. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // Proceedings of the IEEE Symposium on Security and Privacy (S&P). – 2020. – P. 517-533.
3. IEEE Std 802.11-2020. IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems. Local and Metropolitan Area Networks. Part 11: Wireless LAN MAC and PHY Specifications. – IEEE, 2021.
4. WPA3 Specification Version 3.0. – Wi-Fi Alliance, 2020. – 27 p.
5. Steube J. New attack on WPA/WPA2 using PMKID: technical note. – Hashcat Project, 2018.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Диалектика, 2018. – 1040 с.
7. Шевчук П. С. Криптографическая защита информации: учебник. – Москва: РИОР: ИНФРА-М, 2025. – 321 с.