ИССЛЕДОВАНИЕ ВЛИЯНИЯ АТАК НА БЕСПРОВОДНЫЕ СЕТИ WI-FI 6E

М.М. Ковцур*, к.т.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, maxkovzur@mail.ru;*
С.А. Винников, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, vinnikovsema@mail.ru;*
В.И. Трезоров*, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, trezorov.v.i@yandex.ru;*
А.Ю. Кистуга, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, anton.kistruga@gmail.com.*

УДК 004.056.53

Аннотация. В данной работе рассматривается влияние различных атак на функционирование беспроводной сети, работающей на базе стандарта *IEEE* 802.11*ax*. В результате исследования сделан вывод об актуальности некоторых существующих распространенных атак для сетей *Wi-Fi* 6*E*.

Ключевые слова: *Wi-Fi; Wi-Fi* 6*E*; *IEEE* 802.11*ax*; атаки на беспроводные сети.

INVESTIGATION OF THE IMPACT OF ATTACKS ON WI-FI 6E WIRELESS NETWORKS

M.M. Kovtsur, *Ph.D., St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich;*
S.A. Vinnikov, *St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich;*
V.I. Trezorov, *St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich;*
A.Y. Kistruga, *St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich.*

Annotation**.** This paper examines the impact of various attacks on the functioning of a wireless network based on the *IEEE* 802.11*ax* standard. The study concludes the relevance of some existing common attacks to *Wi-Fi* 6*E* networks.

Keywords**:** *Wi-Fi; Wi-Fi* 6*E*; *IEEE* 802.11*ax*; attacks on wireless networks.

Введение

Благодаря развитию мобильных электронно-вычислительных устройств особое распространение получила реализация технологий беспроводной передачи данных, известная как «*Wi-Fi*». *Wi-Fi* частично реализует технологии, описанные в стандарте *IEEE* 802.11 и во множестве поправок к нему. В настоящее время последней широко распространенной поправкой является поправка *IEEE* 802.11*ax*, получившая название «*Wi-Fi* 6*E*». В сетях *Wi-Fi* следует руководствоваться принципами информационной безопасности, которые состоят в обеспечении конфиденциальности и целостности информации, а также доступа к этой информации. Эти принципы могут быть нарушены злоумышленниками, использующими уязвимости указанных беспроводных сетей. В связи с этим вопрос безопасности беспроводных сетей всегда остается актуальным [1].

По статистике Лаборатории Касперского, представленной на рис. 1, за февраль 2023 г. сетевые атаки составили 6% от общего числа киберугроз [2].

Рисунок 1

Количество произведенных устройств, поддерживающих последнее поколение сетей *IEEE* 802.11*ax*, растет с каждым годом (рис. 2) [3]. Изучению беспроводных сетей посвящено достаточно много статей [4-7], однако в них не исследовался стандарт *IEEE* 802.11*ax*. Цель данной работы заключается изучении влияния атак на *Wi-Fi* 6*E*.

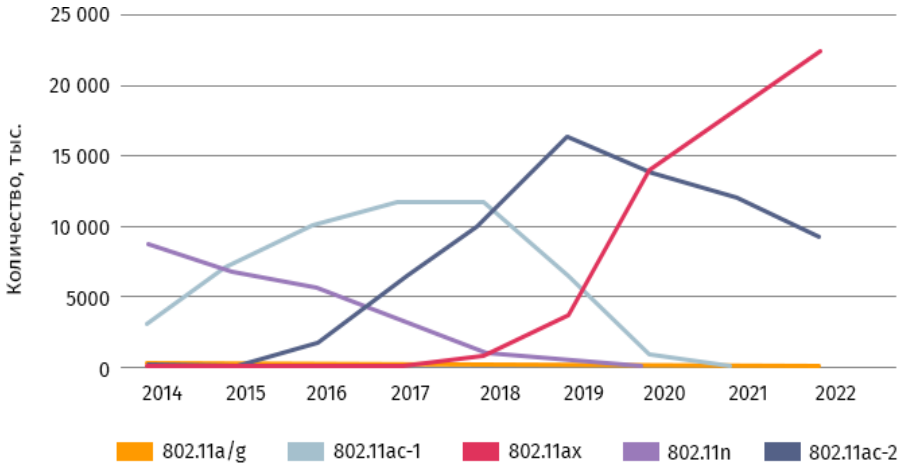

Рисунок 2

Атака деаутентификации

Чтобы выяснить, чем *IEEE* 802.11*ax* отличается от других стандартов *IEEE* 802.11 в контексте безопасности и какие угрозы остались актуальными, следует обратиться к официальному документу от организации *IEEE*. Данный стандарт вводит новый частотный диапазон 6 ГГц и запрещает для него использование некоторых *pre-RSNA* (*WEP, Shared Key Authentication, Open System Authentication without encryption*) и *RSNA* (*WEP, TKIP*) алгоритмов, а также добавляет обязательную защиту кадров управления [8].

Для частотных диапазонов 2,4 ГГц и 5 ГГц в контексте безопасности не было добавлено улучшений, из чего можно сделать предположение, что популярные атаки остаются актуальными для последнего поколения сетей. Чтобы проверить

это, была реализована атака деаутентификации. Выбор атаки обусловлен простотой ее реализации и тем, что она дополняет атаку *Evil Twin* [4].

Принцип действия атаки представлен на рис. 3. Имеется точка доступа и пользователи, которые к ней подключены. Во время атаки злоумышленник отправляет на точку доступа кадры деаутентификации, после чего соединение между клиентами и точкой доступа обрывается. Для подключения требуется повторное прохождение аутентификации. Если отправлять кадры безостановочно, то это вызовет отказ в обслуживании точки доступа [9].

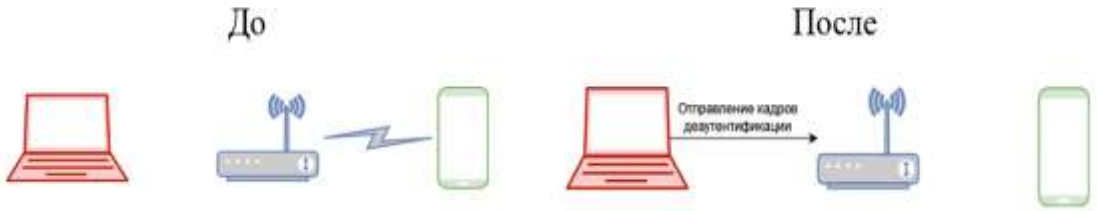

Рисунок 3

Из дампа на рис. 4, видно, что после отправки на точку доступа кадров деаутентификации клиентское устройство заново отправляет кадры аутентификации и ассоциации, что говорит о том, что соединение было разорвано, и атака прошла успешно.

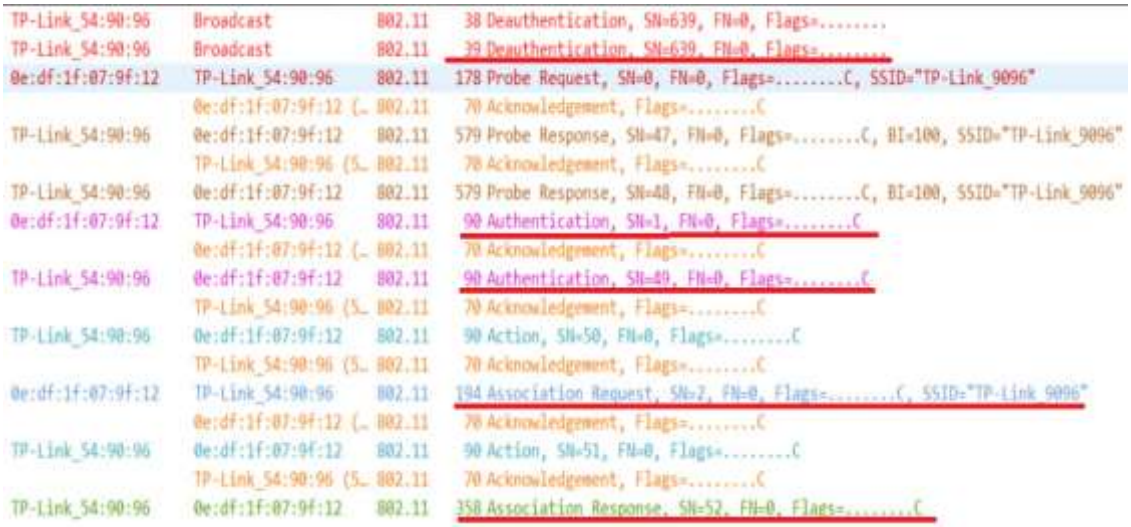

Рисунок 4

Поколение *Wi-Fi* 5 в корпоративных сетях

По данным исследования «Внедрение нового стандарта *Wi-Fi* 6 в России» от «*T*1 Интеграция», *Huawei* и *GlodalCIO*|*DigitalExperts* [10] на момент 2021 г. лишь в 10% организаций было введено новое поколение сетей. Решение о выделении диапазона 5,9-6,4 ГГц в России было принято лишь в декабре 2022 г. Поскольку большая часть корпоративных сетей базируется на *Wi-Fi* 5, новый частотный диапазон 6 ГГц остается недоступным для инфраструктуры. В связи с этим большую угрозу представляют атаки, основанные на создании поддельных точек доступа.

Атака *Evil Twin*

Рисунок 5

На рис. 5 представлена схема атаки «злой двойник». Злоумышленник создает точную копию легитимной точки доступа, к которой в дальнейшем подключается клиент, тем самым давая атакующему доступ к конфиденциальной информации. Атака деаутентификации дополняет злого двойника, вызвав отказ в обслуживании легитимной точки доступа, чтобы пользователь с большей вероятностью подключился к двойнику.

Главная угроза заключается в новом частотном диапазоне. На рынке представлены точки доступа, способные работать на 6 ГГц, также новейшие пользовательские устройства, поддерживающие *Wi-Fi* 6*E*, но как было сказано выше, корпоративное сетевое оборудование не поддерживает данный диапазон, поэтому обнаружить угрозу становится затруднительно.

На данный момент существует три возможных способа обнаружения нелегитимной точки доступа согласно разделу 11 официальной поправки *IEEE* 802.11*ax* [7]:

1. Пассивное сканирование внутри диапазона. Обнаружение кадров *FILS* и незапрашиваемых кадров *Probe Response*. Они представляют из себя уменьшенные маячковые кадры и на их обработку уходит меньше времени (6ГГц).
2. Активное сканирование внутри диапазона. Сканирование предпочтительных каналов (5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 и 229). Выбор каналов обусловлен тем, что они выступают в качестве основного для объединения каналов в 80 МГц (6 ГГц) [11].
3. Обнаружение совместно расположенных точек доступа с помощью *Reduced Neighbor Report* вне диапазона (5 ГГц).

Заключение

Рассмотрена официальная поправка для *Wi-Fi* 6*E* от *IEEE*. Протестирована атака деаутентификации на оборудовании *TP-Link*. Результаты показали, что атаки остаются актуальными для сетей последнего поколения и оказывают негативное влияние на работоспособность. Рассмотрена угроза нового частотного диапазона 6 ГГц: основная проблема заключается в том, что оборудование в корпоративных сетях базируется на *Wi-Fi* 5 и не работает на 6 ГГц. Перечислены способы обнаружения атаки «злой двойник».

Литература

1. Кирилова К.С. Проблема обезвреживания руткитов уровня ядра в системах специального назначения // I-methods, 2020. – Т. 12. – № 3. – С. 1-9.
2. Consumer WLAN Infrastructure // 650 group URL: https://650group.com/reports/consumer-wlan infrastructure/ (дата обращения: 21.02.2023).
3. Serure list // Kaspersky URL: https://statistics.securelist.com/ru/intrusion-detection-scan/month (дата обращения: 28.02.2023).
4. Киструга А.Ю., Ковцур М.М., Оганесян А.Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 485-489.
5. Киструга А.Ю., Ковцур М.М., Петров М.П., Шабанов В.П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция // Сборник науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. – С. 561-564.
6. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning, 2020. – Т. 868. – С. 350-355.
7. Ушаков И.А., Котенко И.В., Овраменко А.Ю., Преображенский А.И., Пелевин Д.В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020. – № 4. – С. 66-71.
8. 802.11ax-2021 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN // IEEE STANDARTS ASSOCIATION URL:https://ieeexplore.ieee.org/document/9442429 (дата обращения: 05.02.2023).
9. Deauthentication // Aircrack-ng URL: http://aircrack-ng.org/doku.php?id=deauthentication (дата обращения: 20.02.2023).
10. T1 Интеграция, Huawei, Global CIO: крупный бизнес не спешит переходить на Wi-Fi 6 // T1 Интеграция URL: https://t1-integration.ru/press/news/t1-integratsiya-huawei-i-global-cio-krupnyy-biznes-ne-speshit-perekhodit-na-wi-fi-6-/(дата обращения: 21.02.2023).
11. Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points // Cisco Live URL: https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2022/pdf/BRKEWN-2024.pdf (дата обращения: 23.02.2023).
12. Ахрамеева К.А., Ворошнин Г.Е., Ковцур М.М. Исследование уязвимостей оборудования mikrotik к атакам на беспроводные сети // X Международная научно-техническая и научно-методическая конференция. Сборник науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. – С. 57-64.
13. Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А., Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности, 2017. – Т. 35. – № 1. – С. 27-30.
14. Юркин Д.В. Системы обнаружения вторжений в сетях широкополосного радиодоступа стандарта IEEE 802.11 // Информационно-управляющие системы, 2014. – № 2 (69). – С. 44-49.

15. Миняев А.А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь, 2020. – № 6. – С. 29-36.
16. Ахрамеева К.А., Ворошнин Г.Е., Ковцур М.М. Исследование устойчивости оборудования mikrotik к атаке association flood на беспроводную сеть семейства ieee 802.11 // Региональная информатика и информационная безопасность.: Сб. трудов. СПб.: СПбГУТ, 2021. – С. 354-358.
17. Герлинг Е.Ю., Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности, 2017. – Т. 35. – С. 27-30.