УЯЗВИМОСТЬ СТАНДАРТОВ WI-FI 802.11 ДЛЯ АТАКИ ДЕАУТЕНТИФИКАЦИИ

А.М. Васюкович, Г.А. Пухир

Современную информационную среду невозможно представить без использования Wi-Fi-технологии. Wi-Fi применяется не только для домашнего пользования, но и в корпоративных сетях. В связи с этим, исследование уязвимостей протокола IEEE 802.11 актуально. Самыми популярными стандартами Wi-Fi на сегодняшний день являются стандарты 802.11b/g/n/ac [1]. Эти стандарты поддерживают все современные устройства и являются основными для подавляющего большинства маршрутизаторов средне/низкого диапазона цены. Однако у этих стандартов существует серьезная уязвимость: подверженность атаке деаутентификации.

Атака деаутентификации – это атака типа «отказ в обслуживании», которая заключается в отправке деаутентификационных фреймов на AP (англ. Access Point – точка доступа) от имени клиента неавторизованным устройством [2]. Такая уязвимость существует из-за того, что эти фреймы при использовании стандартов 802.11b/g/n/ac криптографически не защищены, соответственно, злоумышленнику достаточно узнать MAC-адрес жертвы для реализации атаки. Посредством постоянного повторения атаки, скорость осуществления которой значительно выше скорости повторной авторизации, клиенту можно запретить передачу или получение данных на неопределенный срок.

Существуют несколько способов защиты от данной атаки: использование дорогостоящего оборудования с поддержкой стандарта 802.11w, который обеспечивает шифрование фрейма, однако замедляет скорость Wi-Fi на 20 % [3], или использование нового стандарта шифрования WPA3, что крайне не рекомендуется, из-за найденной

уязвимости Dragon Blood [4]. Кроме этого, существует программы, а также устройства [5], которые позволяют установить факт совершения атаки, однако они не могут локализовать злоумышленника. Следовательно, актуален поиск эффективного способа ее устранения.

Литература

1. Степутин А.Н., Николаев А.Д. Мобильная связь на пути к 6G. В 2 Т. Москва-Вологда: Инфра-Инженерия, 2018. 804 с.
2. Bellado J., Savage S. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions // Proceedings of the 12thUSENIX Security Symposium, Aug 2003, Washington, DC, USA. P. 15–27.
3. Eian M., Mjølsnes S.F. A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities // Proceedings IEEE INFOCOM, March, 2012 in Orlando, Florida, USA. P. 918–926.
4. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // IEEE Symposium on Security and Privacy, 2020. P. 517–533.
5. Горохов Д.Б., Чупин В.Ю. Обнаружение атак типа деаутентификации в сетях стандарта 802.11 с помощью модуля esp8266 // Труды Братского государственного университета. Т.2. Братск, 2019. С. 58–62.