ИССЛЕДОВАНИЕ АТАК AUTHENTICATION FAILURE И ARP INJECT И МЕТОДОВ ИХ ОБНАРУЖЕНИЯ В СЕТЯХ СЕМЕЙСТВА IEEE 802.11

**М. М. Ковцур*, А. Ю. Киструга,
Г. Е. Ворошнин, А. Э. Фёдорова**

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

*Адрес для переписки: maxkovzur@mail.ru

Аннотация—**Предмет исследования.** В наше время технология Wi-Fi используется в мире повсеместно: в офисах крупных компаний, общественных местах и в простых домашних помещениях. Однако использование общедоступной среды передачи приводит к возможности реализации различных атак. В данной статье рассматриваются такие атаки, как authentication failure и Address Resolution Protocol inject. Они показали высокую эффективность и опасность для беспроводных сетей. **Метод.** На первом этапе разобрана концепция работы атак, их основная идея и цель. На последующих этапах, для проведения испытаний, был создан лабораторный стенд, на котором они моделировались. В ходе экспериментов была выяснена эффективность атак, а основные фазы проведения атак и элементы, способствующие их обнаружению, были графически отражены в статье. **Основные результаты.** В результате проделанной работы удалось выделить векторы атак и выявить сопутствующие им аномалии. По материалам исследования были разработаны механизмы обнаружения и предотвращения рассматриваемых атак. **Практическая значимость.** Все теоретические и экспериментальные материалы, собранные в статье, могут быть использованы при обнаружении и предотвращении атак на беспроводные сети сетевыми администраторами и специалистами по информационной безопасности.

Ключевые слова—информационная безопасность, безопасность беспроводных сетей, authentication failure, ARP inject.

Информация о статье
УДК 004.056.5
Язык статьи – русский.
Поступила в редакцию 03.03.2021, принята к печати 24.03.2021.

Ссылка для цитирования: Ковцур М. М., Киструга А. Ю., Ворошнин Г. Е., Фёдорова А. Э. Исследование атак authentication failure и ARP inject и методов их обнаружения в сетях семейства IEEE 802.11 // Информационные технологии и телекоммуникации. 2021. Том 9. № 1. С. 87–98. DOI 10.31854/2307-1303-2021-9-1-87-98.

RESEARCH OF AUTHENTICATION FAILURE AND ARP INJECT ATTACKS AND METHODS OF THEIR DETECTION IN I EEE 802.11 NETWORKS

M. Kovtsur*, A. Kistruga, G. Voroshnin, A. Fedorova

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

*Corresponding author: maxkovzur@mail.ru

Abstract— Nowadays, Wi-Fi technology is used everywhere in the world: in the offices of large companies, public places and in simple home premises. However, the use of a public transmission medium leads to the possibility of various attacks. This article discusses attacks such as authentication failure and Address Resolution Protocol inject. The considered attacks have shown high efficiency and danger for wireless networks. In this connection, methods of detection and protection against them were proposed. Methods. At the first stage, the concept of how attacks work, their main idea and purpose, were analyzed. At the subsequent stages, for testing, a laboratory stand was created, on which they were simulated. In the course of the experiments, the effectiveness of attacks was found out, and the main phases of attacks and the elements that contribute to their detection were graphically reflected in the article. Main results. As a result of the work done, it was possible to isolate attack vectors and identify their accompanying anomalies. Based on the research materials, mechanisms for detecting and preventing the attacks under consideration were developed. The practical part. All theoretical and experimental materials collected in the article can be used in detecting and preventing attacks on wireless networks by network administrators and information security specialists.

Keywords— information security, security of wireless networks, authentication failure, ARP inject.

Article info
Article in Russian.
Received 03.03.2021, accepted 24.03.2021.

For citation: Kovtsur M., Kistruga A., Voroshnin G., Fedorova A.: Research of authentication failure and ARP inject attacks and methods of their detection in IEEE 802.11 networks // Telecom IT. 2021. Vol. 9. Iss. 1. pp. 87–98 (in Russian). DOI 10.31854/2307-1303-2021-9-1-87-98.

Введение

Беспроводные сети широко используются в корпоративном сегменте, однако использование общедоступной среды передачи приводит к возможности реализации различных атак со стороны нелегитимных пользователей. Изучению этих атак посвящены различные исследования [1, 2, 3, 4, 5], однако ряд атак и методов защиты от них для беспроводных сетей исследован крайне мало. К ним относятся атаки authentication failure и ARP INJECT.

Исследование механизма атак

Типовая сеть семейства IEEE 802.11 [6] состоит из точки доступа и подключенных к ней беспроводных клиентов. При рассмотрении атак необходимо ввести понятие злоумышленника - беспроводного клиента, выполняющего атаки, нацеленные на нарушение целостности, доступности сети или конфиденциальности передаваемых данных. В данной статье исследуются атаки Authentication failure и ARP inject.

При рассмотрении атаки Authentication failure обратимся к рис. 1, на котором схематично изображен процесс подключения беспроводного клиента к точке доступа. После успешной аутентификации и ассоциации клиент переходит в состояние 3 и остается в нем, поддерживая беспроводную связь с точкой доступа.

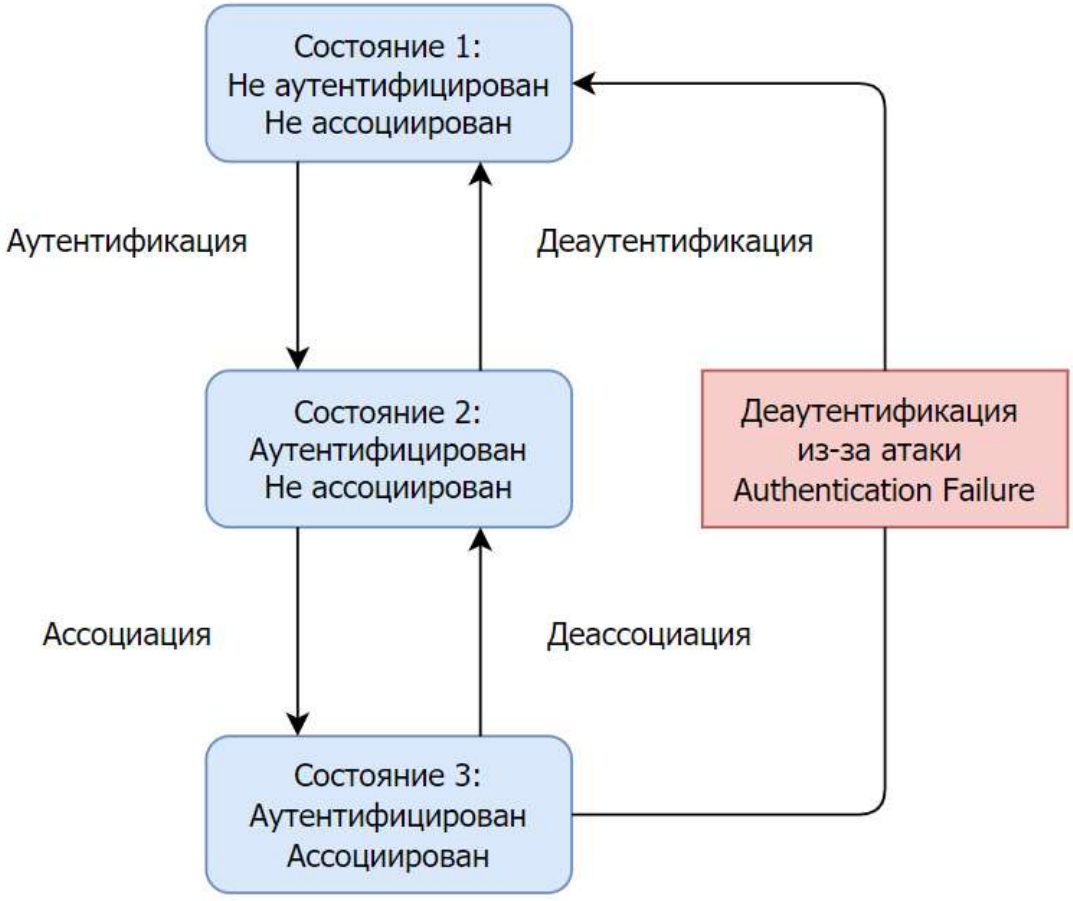

Рис. 1. Механизм атаки Authentication Failure

При проведении данной DoS-атаки злоумышленником подменяются кадры запроса аутентификации от подключенного к точке доступа клиента, находящегося в состоянии 3. В этих кадрах указывается статус код 0x000e, имеющий значение «Received an Authentication frame with authentication transaction sequence number out of expected sequence». Это можно видеть на рис. 2, на котором изображен перехваченный фрейм аутентификации, посылаемый злоумышленником.

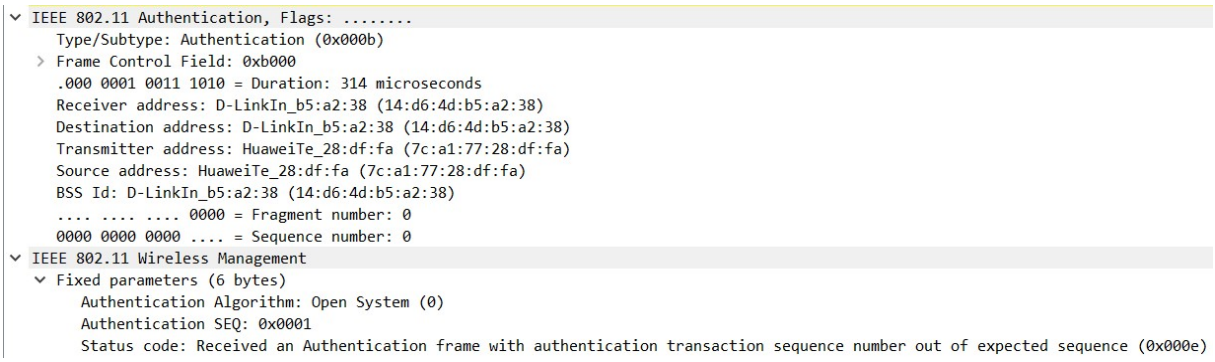

Рис. 2. Содержимое фрейма Authentication злоумышленника

После приема недействительных запросов аутентификации точка доступа обновляет статус клиента до состояния 1, что нарушает взаимодействие клиента и точки доступа. По причине того, что легитимный клиент не являлся инициатором данного взаимодействия, восстановление соединения для него происходит только после получения сообщения деаутентификации с дальнейшим формированием новой сессии. Результатом атаки, во-первых, является кратковременное прерывание обслуживания, приводящее к снижению QoS, а, во-вторых, клиент заново вынужден инициировать 4-х стороннее рукопожатие (4-*way handshake*) в случае использования WPA алгоритмов.

Рассмотрим механизм действия атаки ARP inject. Протокол разрешения адресов (ARP) – это протокол связи, используемый для обнаружения адреса канального уровня, такого как MAC-адрес, связанного с заданным адресом сетевого уровня, обычно адресом IPv4.В связи с тем, что протокол разрешения адресов не защищен, его уязвимость эксплуатируется в атаке ARP inject. Атака, известная так же, как ARP spoofing, нацелена на перенаправление трафика клиента через оборудование злоумышленника. Достигается это путем подмены MAC-адреса в ARP-таблице клиента. Когда клиенту сети необходимо отправить сообщение, но MAC-адрес получателя неизвестен, он отправляет ARP-запрос, в котором указывает IP-адрес станции, обладающей искомым MAC-адресом. Затем, получив ARP-ответ, записывает связку IP – MAC в ARP-таблицу.

В случае с атакой ARP inject реализуется следующий сценарий: злоумышленник, не получая ARP-запросов, отправляет ARP-ответы жертве, подменив в сообщении MAC-адрес основного шлюза на свой. В результате чего клиент, отправляя сообщения в сеть, посылает их вместо основного шлюза злоумышленнику.

Экспериментальная оценка эффективности атак

Для оценки эффективности [7] атак был разработан специализированный стенд. Схема тестирования атаки authentication failure на стенде приведена на рис. 3.

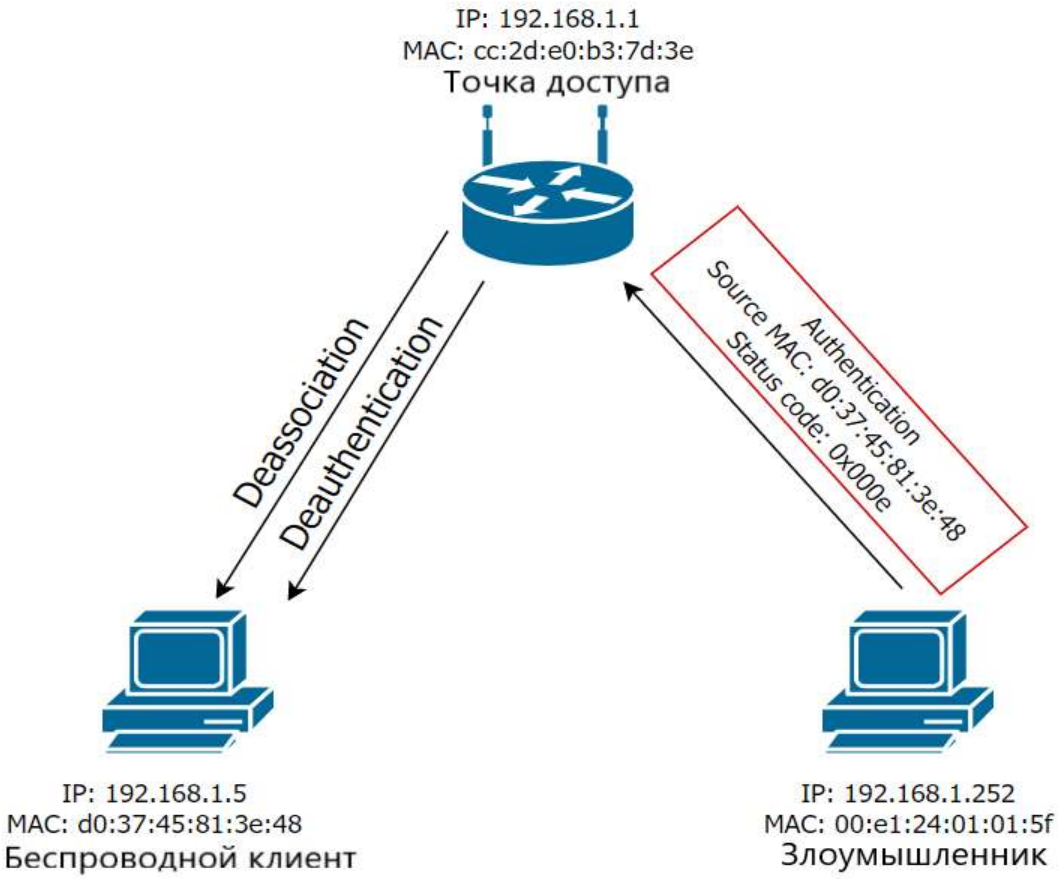

Рис. 3. Схема тестирования эффективности атаки authentication failure

В ходе экспериментальной оценки эффективности атаки с оборудования злоумышленника генерировались кадры с различной частотой. Было определено, что минимальная частота отправки, при которой клиентское устойчиво находится в состоянии 1 или 2, равняется 4 кадрам в секунду. В связи с этим, атаку authentication failure можно считать более эффективной, в сравнении с атакой deauthentication flood. Также важно заметить, что отличительной особенностью по сравнению с обычной атакой деаутентификации является то, что wIDS системы, встроенные в контроллеры или WLAN точки доступа крупнейших производителей не могут идентифицировать подобный тип атаки, т. к. инициатором

деаутентификации является сама точка доступа (автономная или управляемая контроллером)[1, 2, 3]. Это позволяет атакующему оставаться незамеченным.

Для исследования процесса атаки был перехвачен трафик, представленный на рис. 4. После получения фрейма аутентификации с кодом ошибки, точка доступа пытается восстановить связь, отправляя фреймы аутентификации. Но легитимный клиент ничего не отвечает. После нескольких попыток восстановить связь, точка доступа отключает клиента фреймами деассоциации и деаутентификации.

```
HuaweiTe_28:df:fa     D-LinkIn_b5:a2:38     802.11   Authentication, SN=0, FN=0, Flags=........
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Authentication, SN=3187, FN=0, Flags=....R...
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Disassociate, SN=3188, FN=0, Flags=....R...
                      D-LinkIn_b5:a2:38 …   802.11   Acknowledgement, Flags=........
D-LinkIn_b5:a2:38     HuaweiTe_28:df:fa     802.11   Deauthentication, SN=3189, FN=0, Flags=.......
                      D-LinkIn_b5:a2:38 …   802.11   Acknowledgement, Flags=........
```

Рис. 4. Перехваченные кадры атаки Authentication Failure

Схема тестирования атаки ARP inject приведена на рис. 5 (см. след. стр.).

---

[1] Wireless Access Controller (AC and Fit AP) V200R019C10 CLI-based Configuration Guide [Электронный ресурс]. URL: https://support.huawei.com/enterprise/en/doc/EDOC1100156624/4d68bbca/wids-profile (дата обращения: 02.03.2021)

[2] WIPS [Электронный ресурс]. URL: https://docs.ruckuswireless.com/unleashed/200.1.9.12/c-WIPS.html (дата обращения: 02.03.2021)

[3] Cisco Wireless Controller Configuration Guide, Release 8.5 [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/wireless_intrusion_detection_system.html#ids-signatures (дата обращения: 02.03.2021)

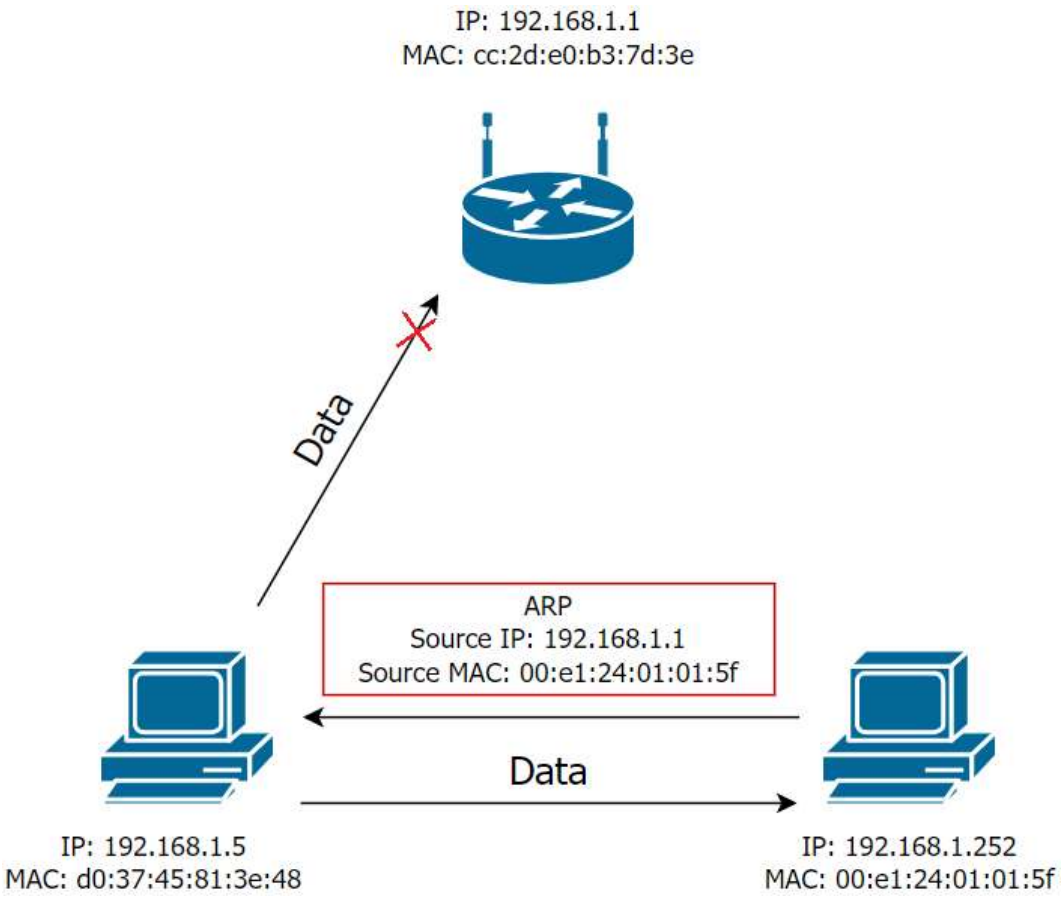

Рис. 5. Схема тестирования эффективности атаки ARP inject

Эффективность данной атаки можно оценить ее успешной реализацией. Для этого рассмотрим атаку на примере. Как можно понять из рис. 6, злоумышленник имеет IP-адрес 172.16.1.252 и MAC-адресом 00.e1.24.01.01.5f. Из рис. 7 и 8, можно увидеть, что MAC-адрес основного шлюза с IP-адресом 172.16.1.1 в ARP-таблице клиента был заменен на MAC-адрес злоумышленника.

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.252  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::9e95:98fd:b66a:5d36  prefixlen 64  scopeid 0x20<link>
        ether 00:e1:24:01:01:5f  txqueuelen 1000  (Ethernet)
        RX packets 8879  bytes 1300435 (1.2 MiB)
        RX errors 0  dropped 2880  overruns 0  frame 0
        TX packets 896  bytes 89325 (87.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 6. Сетевые адреса злоумышленника

```
Интерфейс: 172.16.1.5 --- 0x12
  адрес в Интернете      Физический адрес      Тип
  172.16.1.1             cc-2d-e0-b3-7d-3e     динамический
  172.16.1.252           00-e1-24-01-01-5f     динамический
  239.255.255.250        01-00-5e-7f-ff-fa     статический
```

Рис. 7. ARP-таблица беспроводного клиента до атаки

```
Интерфейс: 172.16.1.5 --- 0x12
  адрес в Интернете      Физический адрес      Тип
  172.16.1.1             00-e1-24-01-01-5f     динамический
  172.16.1.252           00-e1-24-01-01-5f     динамический
  239.255.255.250        01-00-5e-7f-ff-fa     статический
```

Рис. 8. ARP-таблица беспроводного клиента во время атаки

Из рис. 9 и 10 видно, что при трассировке во время атаки в путь сообщений добавляется узел – злоумышленник.

```
C:\Windows\system32>tracert 172.16.1.1

Трассировка маршрута к 172.16.1.1 с максимальным числом прыжков 30

  1     3 ms     3 ms     3 ms  172.16.1.1

Трассировка завершена.
```

Рис. 9. Трассировка IP-адреса основного шлюза до атаки

```
C:\Windows\system32>tracert 172.16.1.1

Трассировка маршрута к 172.16.1.1 с максимальным числом прыжков 30

  1     4 ms     5 ms     2 ms  172.16.1.252
  2     6 ms     3 ms     2 ms  172.16.1.1

Трассировка завершена.
```

Рис. 10. Трассировка IP-адреса основного шлюза во время атаки

Механизмы обнаружения атак authentication failure, ARP inject и защиты от них

На данный момент существует множество методов обнаружения беспроводных атак [8]. В целях обнаружения подобного типа атак следует использовать специализированные системы обнаружения вторжений (wIPS) [9, 10], либо, если оборудование позволяет, разрабатывать свои собственные сигнатуры для детектирования подобного рода атак.

В частности, для детектирования атаки authentication failure следует наблюдать в беспроводной сети кадры аутентификации (тип/подтип 0x000b) со значением 0x0001 и выше в офсете 28 по отношению к началу заголовка канального

уровня (поле *Status Code*, см. табл.[4]). Такие значения встречаются крайне редко при нормальной работе беспроводной сети стандарта IEEE 802.11, и в случае обнаружения подобного кадра система обнаружения вторжений должна предупреждать администратора о подобной активности с целью дальнейшего исследования ситуации.

Таблица.

Статус коды

Статус коды	**Название**	**Значение**
0	SUCCESS	Successful
1	REFUSED, REFUSED_REASON_ UNSPECIFIED	Unspecified failure.
2	TDLS_REJECTED_ALTERNATIVE_PROVIDED	TDLS wakeup schedule rejected but alternative schedule provided.
3	TDLS_REJECTED	TDLS wakeup schedule rejected.
4		Reserved.
5	SECURITY_DISABLED	Security disabled
6	UNACCEPTABLE_LIFETIME	Unacceptable lifetime.
7	NOT_IN_SAME_BSS	Not in same BSS.
8-9		Reserved.
<…>	<…>	<…>

Рассмотрев рис. 11, на котором представлен кадр ARP, посылаемый злоумышленником, можно найти способ обнаружения атаки. А именно, для детектирования атаки ARP inject, следует наблюдать кадры ARP, в которых IP-адрес отправителя соответствует IP-адресу основного шлюза, а MAC-адрес отправителя не соответствует MAC-адресу шлюза.

[4] IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Ac-cess Control (MAC) and Physical Layer (PHY) Specifications // IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012), pp. 731–735, 14 Dec. 2016. DOI 10.1109/IEEESTD.2016.7786995.

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:e1:24:01:01:5f (00:e1:24:01:01:5f)
    Sender IP address: 172.16.1.1
    Target MAC address: Tp-LinkT_81:3e:48 (d0:37:45:81:3e:48)
    Target IP address: 172.16.1.5
```

Рис. 11. Содержимое фрейма ARP-ответа от злоумышленника

При нормальной работе беспроводной сети стандарта IEEE 802.11 такой связки адресов в ARP-сообщении встречаться не может. Следовательно, при детектировании таких фреймов система обнаружения вторжения должна сообщить администратору об атаке ARP inject, проводящейся в его сети.

Заключение

В статье показаны механизмы атак authentication failure и ARP inject. В результате исследования была определена их эффективность и опасность для сети, а также описаны последствия реализации этих атак злоумышленником. После анализа собранных материалов были предложены возможные механизмы обнаружения и предотвращения исследованных атак.

Литература

1. Lovinger N., Gerlich T., Martinasek Z. and Malina L. Detection of wireless fake access points // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2020. pp. 113–118.

2. Alipour H., Al-Nashif Y. B., Satam P. and Hariri S. Wireless anomaly detection based on IEEE 802.11 behavior analysis // IEEE transactions on information forensics and security. 2015. Vol. 10. Iss. 10. pp. 2158–2170. DOI 10.1109/TIFS.2015.2433898.

3. Agarwal M., Purwar S., Biswas S. and Nandi S. Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system // IEEE/CAA Journal of Automatica Sinica. 2016. Vol. 4. Iss. 4. pp. 792–808. DOI 10.1109/JAS.2016.7510178.

4. Kolias C., Kambourakis G., Stavrou A. and Gritzalis S. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset // IEEE Communications Surveys & Tutorials. 2015. Vol. 18. Iss. 1. pp. 184–208. DOI 10.1109/COMST.2015.2402161.

5. Wright J. Detecting wireless LAN MAC address spoofing [Электронный ресурс]. URL: www.uninett.no/wlan/download/wlan-mac-spoof.pdf (дата обращения: 03.02.2021).

6. Данилова Ю. С., Егорова А. Л., Штеренберг С. И. Стандарт беспроводной сети 802.11ax // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. Санкт-Петербург, 26–27 февраля 2020 года. СПб.: Изд-во СПбГУТ, 2020. Т. 1. С. 379–383. ISBN 978-5-89160-197-0.

7. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26–32. DOI 10.46418/2079-8199_2020_3_4

8. Бадамшин М. Р. Проблемы безопасности беспроводных сетей // Международная молодежная научная конференция «XXII Туполевские чтения (школа молодых ученых)»: материалы конференции сборник докладов. Российский фонд фундаментальных исследований, Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ (КНИТУ-КАИ). Казань: Изд-во «Фолиант», 2015. С. 178–182. ISBN 978-5-905576-50-8.

9. Юркин Д. В., Никитин В. Н. Системы обнаружения вторжения в сетях широкополосного радиодоступа стандарта IEEE 802.11 // Информационно управляющие системы. 2014. № 2 (69). С. 44–49.

10. Емельянов А. А., Меркушев О. В. Передача данных в беспроводных сетях IEEE 802.11: угрозы безопасности и методы защиты // Приборостроение в XXI веке – 2015. Интеграция науки, образования и производства : сб. материалов XI Междунар. науч.-техн. конф. (Ижевск, 25–27 нояб. 2015 г.). Ижевск : Изд-во ИжГТУ имени М. Т. Калашникова, 2016. С. 411–419. ISBN 978-5-7526-0742-4.

References

1. Lovinger N., Gerlich T., Martinasek Z. and Malina L. Detection of wireless fake access points // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2020. pp. 113–118.

2. Alipour H., Al-Nashif Y. B., Satam P. and Hariri S. Wireless anomaly detection based on IEEE 802.11 behavior analysis // IEEE transactions on information forensics and security. 2015. Vol. 10. Iss. 10. pp. 2158–2170. DOI 10.1109/TIFS.2015.2433898.

3. Agarwal M., Purwar S., Biswas S. and Nandi S. Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system // IEEE/CAA Journal of Automatica Sinica. 2016. Vol. 4. Iss. 4. pp. 792–808. DOI 10.1109/JAS.2016.7510178.

4. Kolias C., Kambourakis G., Stavrou A. and Gritzalis S. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset // IEEE Communications Surveys & Tutorials. 2015. Vol. 18. Iss. 1. pp. 184–208. DOI 10.1109/COMST.2015.2402161.

5. Wright J. Detecting wireless LAN MAC address spoofing. URL: www.uninett.no/wlan/download/wlan-mac-spoof.pdf (03.02.2021).

6. Danilova U., Egorova A., Shterenberg S. 802.11AX wireless network standard // Aktualnye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2020) : IX Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya : sb. nauch. st. v 4-h t. Sankt-Peterburg, 26–27 fevralya 2020 goda. SPb.: Izd-vo SPbGUT, 2020. T. 1. pp. 379–383 (in Russian). ISBN 978-5-89160-197-0.

7. Minyaev A. A., Krasov A. V. The methodology of efficiency assessment of protection system of distributed information systems // Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and technical science. 2020. Iss. 3. pp. 26–32 (in Russian). DOI 10.46418/2079-8199_2020_3_4

8. Badamshin M. R. Problemy bezopasnosti besprovodnyh setej // Mezhdunarodnaya molodezhnaya nauchnaya konferenciya «XXII Tupolevskie chteniya (shkola molodyh uchenyh)»: materialy konferencii sbornik dokladov. Rossijskij fond fundamental'nyh issledovanij, Kazanskij nacional'nyj issledovatel'skij tekhnicheskij universitet im. A. N. Tupoleva-KAI (KNITU-KAI). Kazan': Izd-vo "Foliant", 2015. S. 178–182 (in Russian). ISBN 978-5-905576-50-8.

9. Yurkin D. V., Nikitin V. N. Intrusion detection systems in IEEE 802.11 local wireless networks // Information and control systems. 2014. Iss. 2 (69). pp. 44–49 (in Russian).

10. Emelyanov A. A., Merkushev O. V. Data transmission in wireless networks of IEEE 802.11 standard: security threats and protection methods // Priborostroenie v XXI veke – 2015. Integraciya nauki, obrazova-niya i proizvodstva : sb. materialov XI Mezhdunar. nauch.-tekhn. konf. (Izhevsk, 25–27 noyab. 2015 g.). Izhevsk : Izd-vo IzhGTU imeni M. T. Kalashnikova, 2016. S. 411–419 (in Russian). ISBN 978-5-7526-0742-4.

Ковцур Максим Михайлович
кандидат технических наук, доцент кафедры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@gmail.com

Кистружа Антон Юрьевич
инженер, anton.kistruga@gmail.com

Ворошнин Григорий Евгеньевич
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voroshnin.g@gmail.com

Фёдорова Анастасия Эдуардовна
студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fyodorova.aaee@gmail.com

Kovtsur Maxim M.
candidate of engineering sciences, associate professor, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, maxkovzur@gmail.com

Kistruga Anton Yu.
engineer, anton.kistruga@gmail.com

Voroshnin Grigoriy E.
student, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, voroshnin.g@gmail.com

Fedorova Anastasija E.
student, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, fyodorova.aaee@gmail.com