Wireless Internet Project - MAC Randomization

Edoardo Saputelli - Francesca De Donato

July 2022

1 Project overview

1.1 Technical introduction

The project was focused on the analysis of the active scanning process of different devices, evaluating how their behaviour changes according to different conditions.

When a device wants to connect to an Access Point located nearby, it performs the active scanning process. It consists in the emission of a certain type of managements frames, called Probe Requests.

However, differently from most other packets sent across the network, Probe Requests are emitted in-the-clear, giving the possibility to be sniffed very easily through the use of specific tools, like Wireshark.

Since it could result as a serious attempt to the privacy of the users, MAC randomization techniques were developed to solve this issue. This is an important countermeasure since, in general, MAC addresses uniquely identify electronic devices, leading to a very easy tracking of the owner of a specific device through the analysis of its Probe Requests.

1.2 What we did

To pursue the goal of analyzing the randomization behaviour of the chosen devices, we followed the procedures employed in the paper "A dataset of labelled device Wi-Fi probe requests for MAC address de-randomization" by L. Pintor and L. Aztori, Computer Networks, Vol. 205, March 2022.

The authors of the paper evaluated how each analyzed device changed its way of emitting Probe Requests depending on its settings, which consist in a combination of screen on/off, Wi-Fi on/off, power saving on/off.

In particular, six circumstances were examined:

- A: Screen on, Wi-Fi on, power saving off;
- S: Screen off, Wi-Fi on, power saving off;
- PA: Screen on, Wi-Fi on, power saving on;

- PS: Screen off, Wi-Fi on, power saving on;
- WA: Screen on, Wi-Fi off, power saving off;
- WS: Screen off, Wi-Fi off, power saving off.

However, we noticed that, during the analysis of each device, the opening of its Wi-Fi settings caused an increase in the number of the Probe Requests sent by it (in particular, it happened with the interface where the user can choose the available Wi-Fi networks). For this reason, it could be interesting to analyze another circumstance:

- IF: Screen on (on Wi-Fi interface), Wi-Fi on, power saving off.

2 Technical part

The analysis of the packets sent across the network was performed through the Wireshark tool set in Monitor mode, within the Live version of the Kali Linux operating system.

In order to perform the analysis in an isolated area, all the nearby devices were set to airplane mode.

In all the above-mentioned circumstances, each analysis lasted 20 minutes.

All the packets retrieved during each analysis have been filtered on Wireshark to be Probe Requests.

Evaluating a device at a time, it has been easy to identify the packets sent by the device in question. Indeed, in order to filter out all the other devices in the area, it was important to consider that the device under analysis was the nearest one to the laptop which performed the sniffing. For this reason, the device has always been recognized as the one with the strongest emitted signal, i.e. the highest RSSI (Receive Signal Strenght Indicator) parameter, in general resulting as a value ≥ -40 dBm.

This project was mainly focused on the randomization behaviour of the devices under analysis. For this purpose, the way to recognize if a MAC address is randomized consists in evaluating the second bit of the first byte of the address: if it is equal to 1 it means that the MAC address is randomized.

2.1 Device 1: iPhone 7

The first device to be evaluated was an iPhone 7 (operating system: iOS, version 14.6).

The 20min analysis of the above-mentioned circumstances brought to the following results:

- A: 38 packets, 14 MAC address, 0 real MAC addresses;
- S: 7 packets, 1 MAC address, 0 real MAC addresses;
- PA: 49 packets, 19 MAC addresses, 0 real MAC addresses;

- PS: 1 packets, 1 MAC address, 0 real MAC addresses;
- WA: 0 packets;
- WS: 0 packets;
- IF: 379 packets, 150 MAC addresses, 0 real MAC addresses.

Setting S:

No.	Time	Source	Destination	Protocol	Length	RSSI	Info
1	0.000000	fa:72:0e:f5:f6:36	Broadcast	802.11	221	-30 dBm	Probe Request, SN=3951, FN=0, Flags=........C, SSID=eduroam
2	0.045215	fa:72:0e:f5:f6:36	Broadcast	802.11	230	-30 dBm	Probe Request, SN=3956, FN=0, Flags=........C, SSID=polimi-protected
3	0.046906	fa:72:0e:f5:f6:36	Broadcast	802.11	221	-30 dBm	Probe Request, SN=3957, FN=0, Flags=........C, SSID=eduroam
4	0.047826	fa:72:0e:f5:f6:36	Broadcast	802.11	148	-32 dBm	Probe Request, SN=3958, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
5	0.067608	fa:72:0e:f5:f6:36	Broadcast	802.11	230	-33 dBm	Probe Request, SN=3959, FN=0, Flags=........C, SSID=polimi-protected
6	0.078496	fa:72:0e:f5:f6:36	Broadcast	802.11	221	-33 dBm	Probe Request, SN=3960, FN=0, Flags=........C, SSID=eduroam
7	0.079356	fa:72:0e:f5:f6:36	Broadcast	802.11	148	-33 dBm	Probe Request, SN=3961, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

Setting PS:

No.	Time	Source	Destination	Protocol	Length	RSSI	Info
1	0.000000	2a:ec:39:5b:ed:8e	Broadcast	802.11	148	-25 dBm	Probe Request, SN=3320, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

The results show that the iPhone 7 didn't send any Probe Request during the Wi-Fi off settings and that it changed quite often its MAC address, never using its real one.

Instead, focusing on the Wi-Fi switched on circumstances, it is trivial to notice that PS is the one in which less packets are sent (just one within a 20 minutes interval!). On the other hand, the IF setting detected a really huge number of Probe Requests sent across the network, greater by far with respect to the other evaluated settings. Finally, differently from what expected for the screen active circumstances, it is easy to see that this device sent more packets with the power saving mode on than with this functionality switched off.

2.2 Device 2: iPhone 13 Pro

The second device to be evaluated was an iPhone 13 Pro (operating system: iOS, version 15.4.1).

The 20min analysis of the above-mentioned circumstances brought to the following results:

- A: 36 packets, 23 MAC addresses, 0 real MAC addresses;
- S: 75 packets, 47 MAC addresses, 0 real MAC addresses;
- PA: 65 packets, 41 MAC addresses, 0 real MAC addresses;
- PS: 61 packets, 41 MAC addresses, 0 real MAC addresses;
- WA: 0 packets;
- WS: 0 packets;
- IF: 248 packets, 145 MAC addresses, 0 real MAC addresses;

Setting A:

No.	Time	Source	Destination	Protocol	Length	RSSI	Info
1	0.000000	52:1d:0a:6e:ae:88	Broadcast	802.11	173	-33 dBm	Probe Request, SN=4070, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
2	0.020389	52:1d:0a:6e:ae:88	Broadcast	802.11	173	-32 dBm	Probe Request, SN=2138, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
3	12.812742	da:72:db:59:6f:03	Broadcast	802.11	173	-30 dBm	Probe Request, SN=447, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
4	12.832965	da:72:db:59:6f:03	Broadcast	802.11	173	-30 dBm	Probe Request, SN=448, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
5	28.966412	a2:54:c5:95:a4:0b	Broadcast	802.11	173	-30 dBm	Probe Request, SN=491, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
6	29.098903	e6:1b:40:95:73:9d	Broadcast	802.11	173	-31 dBm	Probe Request, SN=3114, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
7	29.172479	9a:6b:a6:8c:19:86	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1269, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
8	29.192754	9a:6b:a6:8c:19:86	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1271, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
9	36.021664	ee:8a:dd:af:7f:5e	Broadcast	802.11	173	-31 dBm	Probe Request, SN=3016, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
10	36.041934	ee:8a:dd:af:7f:5e	Broadcast	802.11	173	-30 dBm	Probe Request, SN=3017, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
11	47.376202	c2:39:c7:d2:eb:38	Broadcast	802.11	173	-30 dBm	Probe Request, SN=2133, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
12	47.396481	c2:39:c7:d2:eb:38	Broadcast	802.11	173	-29 dBm	Probe Request, SN=1845, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
13	47.750548	9a:c4:ba:18:8e:55	Broadcast	802.11	173	-30 dBm	Probe Request, SN=3635, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
14	47.770900	9a:c4:ba:18:8e:55	Broadcast	802.11	173	-30 dBm	Probe Request, SN=3636, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
15	81.444774	52:fa:4f:86:2b:3d	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1437, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
16	81.819407	5e:6b:5b:ab:d3:d9	Broadcast	802.11	173	-31 dBm	Probe Request, SN=2750, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
17	81.865876	2e:6a:77:71:a7:bd	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1818, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
18	81.886044	2e:6a:77:71:a7:bd	Broadcast	802.11	173	-32 dBm	Probe Request, SN=1819, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
19	114.371301	3e:0b:d4:12:23:e4	Broadcast	802.11	173	-31 dBm	Probe Request, SN=3879, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
20	114.464644	a2:5c:da:e9:fe:98	Broadcast	802.11	173	-31 dBm	Probe Request, SN=2159, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
21	114.485006	a2:5c:da:e9:fe:98	Broadcast	802.11	173	-32 dBm	Probe Request, SN=2160, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
22	168.851515	ce:71:9f:99:eb:1a	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1807, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
23	176.536840	72:d7:0a:c2:4a:bc	Broadcast	802.11	173	-30 dBm	Probe Request, SN=3205, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
24	176.675716	46:01:15:9e:d1:fb	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1196, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
25	176.696162	46:01:15:9e:d1:fb	Broadcast	802.11	173	-31 dBm	Probe Request, SN=2070, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
26	176.769622	46:cc:b5:0a:5f:d1	Broadcast	802.11	173	-30 dBm	Probe Request, SN=4083, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
27	176.789710	46:cc:b5:0a:5f:d1	Broadcast	802.11	173	-30 dBm	Probe Request, SN=4084, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
28	293.262665	ea:29:f6:32:28:3f	Broadcast	802.11	173	-32 dBm	Probe Request, SN=2317, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
29	293.282778	ea:29:f6:32:28:3f	Broadcast	802.11	173	-32 dBm	Probe Request, SN=1593, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
30	293.768458	0a:b4:aa:0d:1b:c7	Broadcast	802.11	173	-31 dBm	Probe Request, SN=2507, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
31	540.573315	ca:5f:78:2a:ed:f3	Broadcast	802.11	173	-32 dBm	Probe Request, SN=1560, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
32	540.778611	8e:99:69:92:a3:08	Broadcast	802.11	173	-32 dBm	Probe Request, SN=3267, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
33	540.798887	8e:99:69:92:a3:08	Broadcast	802.11	173	-33 dBm	Probe Request, SN=3269, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
34	1053.361259	e6:b6:5c:35:bd:90	Broadcast	802.11	173	-31 dBm	Probe Request, SN=1091, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
35	1053.892497	e6:18:32:af:f2:2b	Broadcast	802.11	173	-34 dBm	Probe Request, SN=1388, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
36	1053.912782	e6:18:32:af:f2:2b	Broadcast	802.11	173	-33 dBm	Probe Request, SN=1389, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

As the other device, the iPhone 13 Pro didn't send any packet while keeping the Wi-Fi turned off. However, with respect to the iPhone 7, it sent a greater (by far) amount of Probe Requests within the S and PS settings, i.e. keeping the Wi-Fi active but the screen switched off. Finally, it is trivial to notice that, also in this case, the IF setting was the one that detected the greatest number of packets sent across the network.

3 Conclusions

The captures performed during this project highlighted the analogies and the differences between the two examined devices.

Indeed, from the carried out experiments, it is trivial to observe how none of them sent packets while keeping the Wi-Fi turned off (settings WA and WS).

However, it can be noticed that the iPhone 13 Pro sent on average more Probe Requests than the previously analyzed iPhone 7 (with the exception of the IF circumstance). Moreover, the captures show how the iPhone 13 Pro seems more inclined to randomize its MAC address, but in particular to send packets while keeping the Wi-Fi turned on but the screen off (S and PS settings).

In particular, as mentioned during the report introduction, it can be easily observed for both the devices that the circumstance in which Probe Requests are sent more frequently is the IF one, i.e. with the device kept opened on its Wi-Fi settings.