Wireless Internet

# Analyzing MAC Address Randomization in Wi-Fi Probe Requests

Seyedmohammad Tabatabaei 10967133
Iman Javaheri Neyestanak 10976128

## 1. Introduction

In this report, we study how the iPhone 12 and Samsung A31smartphones use MAC address randomization in their Wi-Fi probe requests. To do this, we used a sniffer in monitor mode along with Wireshark to capture and examine the probe request packets. We performed the experiment in different scenarios to better understand how the devices behave when sending probe requests.

| | |
|---|---|
| iPhone 12 | 20:32:C6:E2:E1:C4 |
| Samsung A31 | B4:1A:1D:3C:24:E7 |

Probe requests are used by devices to look for Wi-Fi networks before connecting. These requests often include a MAC address, which can be randomized to improve user privacy. By randomizing the MAC address, the device makes it harder for third parties to track the user's real identity.

In this project, we focused on identifying any patterns in the MAC addresses during probe requests and checked how often and how well they were randomized. The main aim was to understand how each of these two devices handles MAC randomization, and how effective these methods are in protecting the user's privacy.

The results of our study give useful information about the privacy techniques used in these smartphones and show the differences in how each brand implements MAC address randomization.

## 2. Procedure

The sniffing process was carried out using a MacBook set in monitor mode with the Wireshark software. The experiment was done in a controlled environment using two smartphones: the iPhone 12 and the Samsung A31. Packet sniffing was performed on a single Wi-Fi channel, specifically channel 2, with a bandwidth of 20 MHz.

To ensure close distance between the access point and the station, the roles of the two phones were exchanged during the tests. One phone acted as the access point, while the other worked as the station, and then they were switched.

The following device states were considered to evaluate the MAC address randomization behavior of the two smartphones:

| Mode | Active screen on | Wi-fi on | Power saving on |
|---|---|---|---|
| A | X | X | |
| S | | X | |
| PA | X | X | X |
| PS | | X | X |
| WA | X | | |
| WS | | | |

**Table 1. Device modes ( “X” means that the relevant mode is “on”).**

To focus specifically on probe requests and separate them from other network traffic, a two-step filtering process was applied after the data capture.

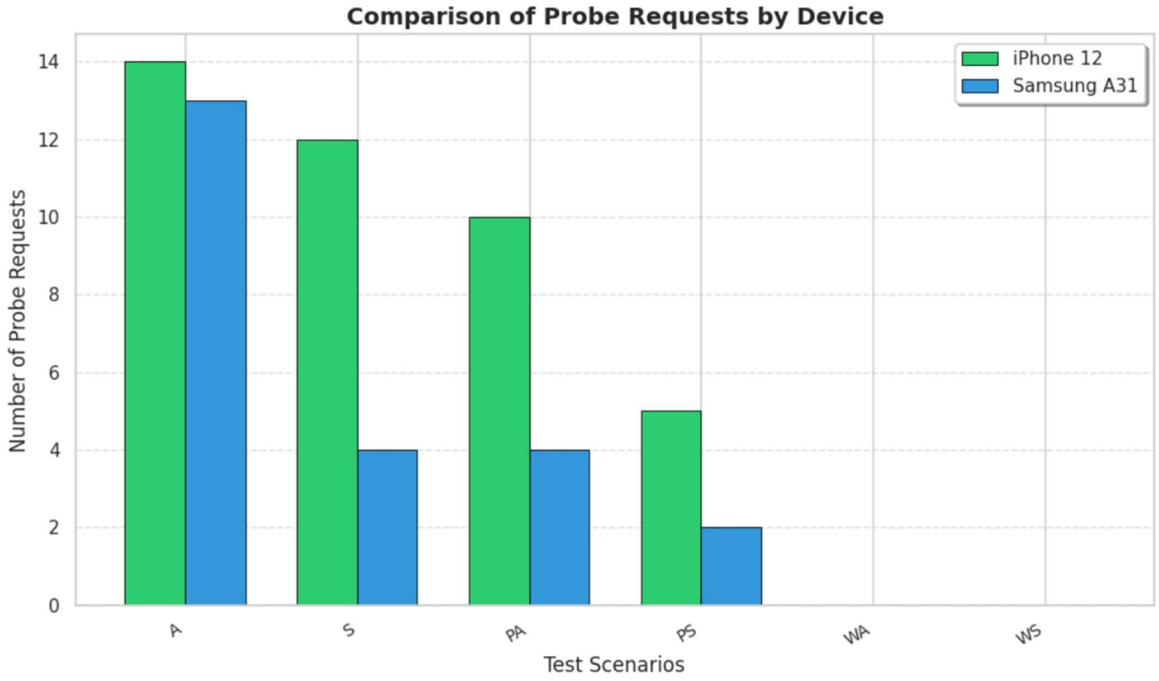
To identify packets related to probe requests, the filter `wlan.fc.type_subtype == 0x0004` was applied. This filtering step removed unrelated packets, allowing us to focus specifically on the probe requests sent by the devices.

To ensure that only probe requests from the target devices were analyzed, signal strength was used as an additional filter. Specifically, we applied the condition wlan_radio.signal_dbm >= -55 to capture packets from devices located within close range—approximately 20 cm from the sniffer. This approach helped eliminate background noise from other nearby devices and ensured higher accuracy in the results.

A total of 12 scenarios were tested for both the iPhone 12 and the Samsung A31. By focusing on probe requests with stronger signal strength, the dataset was limited to the transmissions most likely originating from the two smartphones under study.

3. Results

During the examination of MAC address randomization in probe requests, unique address patterns were identified for both the iPhone 12 and the Samsung A31. The data, collected via a MacBook and analyzed using Wireshark, is illustrated below. This figure highlights the differences in MAC address assignment strategies used by the two devices when attempting to connect to Wi-Fi networks.




4. Conclusion

In conclusion, this report examined the MAC address randomization behavior in Wi-Fi probe requests for the iPhone 12 and Samsung A31across various scenarios conducted in a controlled environment. The findings revealed that MAC randomization patterns differ depending on the device's state and manufacturer policies. The highest frequency of probe requests occurs when both the Wi-Fi and screen are active. This number decreases noticeably when the screen is turned off, and no probe requests are detected when the Wi-Fi is disabled. Additionally, power-saving features further reduce network activity, leading to the lowest number of probe requests during power-saving mode combined with the screen being off.

The results improve our knowledge of the impact that device status and power-saving settings have on the behavior of probe requests. Moreover, they offer valuable information

about the privacy mechanisms implemented by the devices when connecting to Wi-Fi networks, especially emphasizing how MAC randomization contributes to strengthening user privacy.