MAC address randomization

draft-ietf-mac-address-randomization-02

IETF 114 – MADINAS WG

Juan Carlos Zúñiga – CISCO
Carlos J. Bernardos – UC3M
Amelia Andersdotter – Sky UK

July 2022

Introduction and goals

- Privacy, an increasing concern
  - Layer-2 globally unique identifiers (MAC addresses) have been assigned to devices and are transmitted in the clear in, for instance, beacons, probe requests, or after association
  - MAC addresses can easily be intercepted and used to track location or behavior
- Several projects in IETF, IEEE 802 and among mobile OS vendors to deal with plain-text, unique, permanent MAC addresses
  - Assigning a random MAC address to a device per connection, per SSID, after some time period
  - Area of extensive research (see reference Martin et al (2017) in draft for more comprehensive list of research in this area, or IEEE 802.11 RCM TIG final report in 11-19/1442r9, also in draft)
- Goal of this draft: document Current State of Affairs regarding MAC address randomization

Table of contents

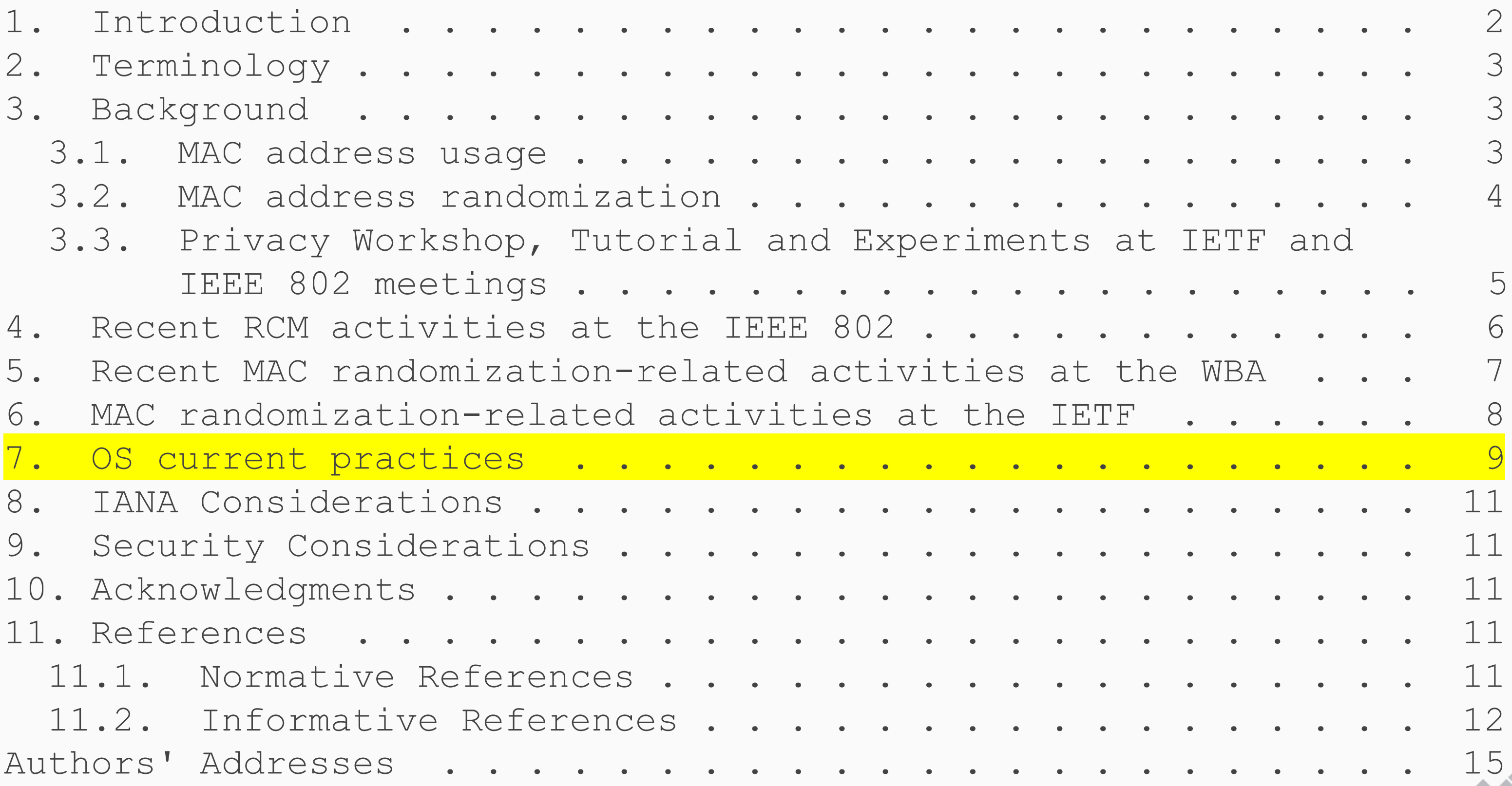
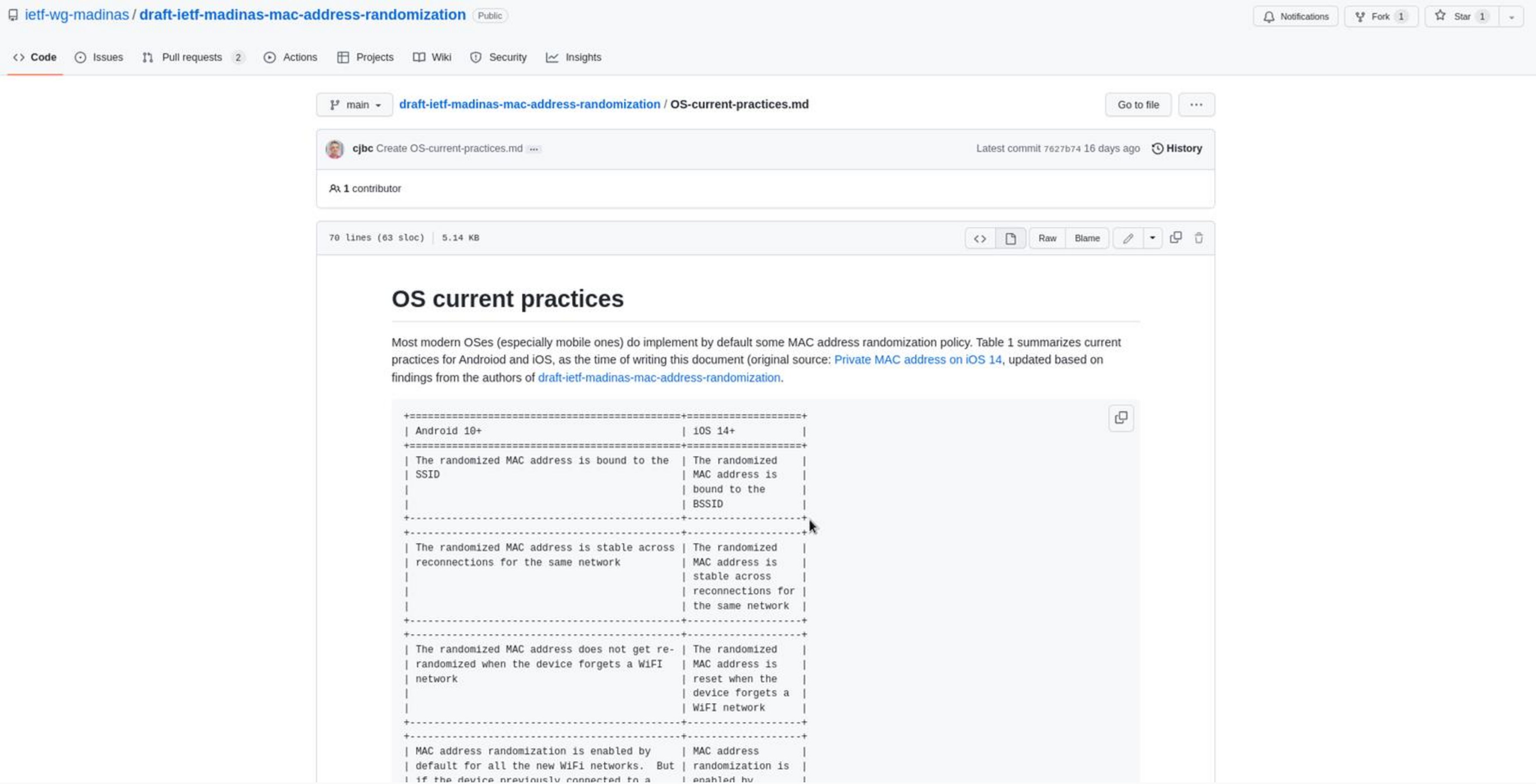


Table of contents

Since this content can evolve with time, it is now hosted at https://github.com/ietf-wg-madinas/draft-ietf-madinas-mac-address-randomization/blob/main/OS-current-practices.md

Table of contents


ietf-wg-madinas / draft-ietf-madinas-mac-address-randomization Public
Notifications
Fork 1
Star 1
Code
Issues
Pull requests 2
Actions
Projects
Wiki
Security
Insights
main
draft-ietf-madinas-mac-address-randomization / OS-current-practices.md
Go to file
cjbc Create OS-current-practices.md
Latest commit 7627b74 16 days ago
History
1 contributor
70 lines (63 sloc) | 5.14 KB
Raw
Blame

OS current practices

Most modern OSes (especially mobile ones) do implement by default some MAC address randomization policy. Table 1 summarizes current practices for Androiod and iOS, as the time of writing this document (original source: Private MAC address on iOS 14, updated based on findings from the authors of draft-ietf-madinas-mac-address-randomization.

```
+=============================================+===================+
| Android 10+                                 | iOS 14+           |
+=============================================+===================+
| The randomized MAC address is bound to the  | The randomized    |
| SSID                                        | MAC address is    |
|                                             | bound to the      |
|                                             | BSSID             |
+---------------------------------------------+-------------------+
+---------------------------------------------+-------------------+
| The randomized MAC address is stable across | The randomized    |
| reconnections for the same network          | MAC address is    |
|                                             | stable across     |
|                                             | reconnections for |
|                                             | the same network  |
+---------------------------------------------+-------------------+
+---------------------------------------------+-------------------+
| The randomized MAC address does not get re- | The randomized    |
| randomized when the device forgets a WiFI   | MAC address is    |
| network                                     | reset when the    |
|                                             | device forgets a  |
|                                             | WiFI network      |
+---------------------------------------------+-------------------+
+---------------------------------------------+-------------------+
| MAC address randomization is enabled by     | MAC address       |
| default for all the new WiFi networks.  But | randomization is  |
| if the device previously connected to a     | enabled by        |
```

MAC randomization-related activities at the IETF

- Early work as far as back as IETF91
    - Joint W3C/IAB privacy tutorial
    - Testing MAC randomization and technical features (i.e., collisions, DHCP, etc.)
    - Thoroughly documented

- Led/linked to a number of other initiatives (see draft), e.g., RFC7217, RFC8947, RFC8948

- MAC randomization is now a default privacy feature in major mobile OSes (see later slide)

Recent RCM activities at the IEEE 802

- IETF work inspired a new privacy research project, P802E

- Discussions about randomized MAC for different types of devices (industrial, sensors, personal, etc.) in e.g., 802C (“SLAP”)

- Currently, two task groups in IEEE 802.11 are dealing with issues related to Randomized and Changing MAC addresses (RCM)

Juan Carlos has updated us today on this

Recent MAC randomization-related activities at the WBA

- The Wireless Broadband Alliance (WBA), the Testing and Interoperability Work Group has been looking at the issues related to MAC address randomization

- WBA has documented a set of use cases that a Wi-Fi Identification Standard should address in order to scale and achieve longer term sustainability of deployed services

OS current practices

Android 10+	iOS 14+
The randomized MAC address is bound to the SSID	The randomized MAC address is bound to the BSSID
The randomized MAC address is stable across reconnections for the same network	The randomized MAC address is stable across reconnections for the same network
The randomized MAC address does not get re-randomized when the device forgets a WiFI network	The randomized MAC address is reset when the device forgets a WiFI network
MAC address randomization is enabled by default for all the new WiFi networks. But if the device previously connected to a WiFi network identifying itself with the real MAC address, no randomized MAC address will be used (unless manually enabled)	MAC address randomization is enabled by default for all the new WiFi networks

OS current practices

OS	Linux	Android 10	Windows 10	iOS 14+
Random per net.	Y	Y	Y	Y
Random per connec.	Y	N	N	N
Random daily	N	N	Y	N
SSID config.	Y	N	N	N
Random. for scan	Y	Y	Y	Y
Random. for scan by default	N	Y	N	Y

**Starting in Android 12, Android uses non-persistent randomization in the following situations: (i) a network suggestion app specifies that non-persistent randomization be used for the network (through an API); or (ii) the network is an open network that hasn't encountered a captive portal and an internal config option is set to do so (by default it is not)

Changelog

- -ietf-*-00:
  - Adopted version

- -ietf-*-01:
  - Addressed comments from Hai Shalom

- -ietf-*-02:
  - Move section 7 (OS current practices) to GitHub