

MAC address randomization

draft-ietf-mac-address-randomization-02

20221007 interim – MADINAS WG

Juan Carlos Zúñiga – CISCO

Carlos J. Bernardos – UC3M

Amelia Andersdotter – Sky UK

October 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

1.	Introduction	2
2.	Terminology	3
3.	Background	3
3.1.	MAC address usage	3
3.2.	MAC address randomization	4
3.3.	Privacy Workshop, Tutorial and Experiments at IETF and IEEE 802 meetings	5
4.	Recent RCM activities at the IEEE 802	6
5.	Recent MAC randomization-related activities at the WBA	7
6.	MAC randomization-related activities at the IETF	8
7.	OS current practices	9
8.	IANA Considerations	11
9.	Security Considerations	11
10.	Acknowledgments	11
11.	References	11
11.1.	Normative References	11
11.2.	Informative References	12
	Authors' Addresses	15



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 Android 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 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	MAC address randomization is enabled by

Comments received

Michael Richardson

- “Both documents have BCP14 terminology, but no keywords used.”
 - We will remove the terminology section in version -03
- “If there is some goal of explaining why we have the problem, then maybe section 3 of mac-address-randomization should also show an 802.11 header, showing where the EUI show up, and why they are not, and can not, be encrypted.”
 - We believe we should not get into that level of details, and rather focus on the MAC address format and issues. We can though add some text about the encryption.

Comments received

Michael Richardson (cont'd)

- Sent several git pull requests, one about creating a taxonomy section
 - ## Per-Vendor OUI MAC address (PVOM)
 - ## Per-Device Generated MAC address (PDGM)
 - ## Per-Boot Generated MAC address (PBGGM)
 - ## Per-Network Generated MAC address (PNGM)
 - ## Per-Session Generated MAC address (PSGM)
 - ## Per-Period Generated MAC address (PPGM)

Comments received

Per-Device Generated MAC address (PDGM)

This form of MAC address is randomly generated by the device, usually upon first boot.

The resulting MAC address is stored in non-volatile storage and is used for the rest of the device lifetime.

Per-Boot Generated MAC address (PBGM)

This form of MAC address is randomly generated by the device, each time the device is booted.

The resulting MAC address is **not** stored in non-volatile storage.

It does not persist across power cycles.

This case may sometimes be a PDGM where the non-volatile storage is no longer functional (or has failed).

Comments received

Per-Network Generated MAC address (PNGM)

This form of MAC address is generated each time a new network connection is created.

This is typically used with WiFi (802.11) networks where the network is identified by an SSID Name.

The generated address is stored on non-volatile storage, indexed by the SSID.

Each time the device returns to a network with the same SSID, the device uses the saved MAC address.

It is possible to use PNGM for wired ethernet connections through some passive observation of network traffic, such as STP, LLDP, DHCP or Router Advertisements to determine which network has been attached.

Per-Session Generated MAC address (PSGM)

This form of MAC address is generated each time a new network connection is created.

Like PNGM, it is used primarily with WiFi (802.11).

The generated address is not stored on non-volatile storage, nor in any in-device database.

Should the device disconnect from that SSID and then reconnect, a new MAC address will be generated.

As there are often small interruptions in hand-over between access points, this MAC address usually needs to be kept for short times.



Comments received

Per-Period Generated MAC address (PPGM)

This form of MAC address is generated periodically.

Typical numbers are around every twelve hours.

Like PNGM, it is used primarily with WiFi (802.11).

When the MAC address changes, the station disconnects from the current session and reconnects using the new MAC address.

This will involve a new WPA/802.1x session: new EAP, TLS, etc. negotiations.

A new DHCP, Router-Advertisement will be done.

If DHCP is used, then a new DUID is generated so as to not link to the previous connection, and the result is usually new IP addresses allocated.

Next steps?