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

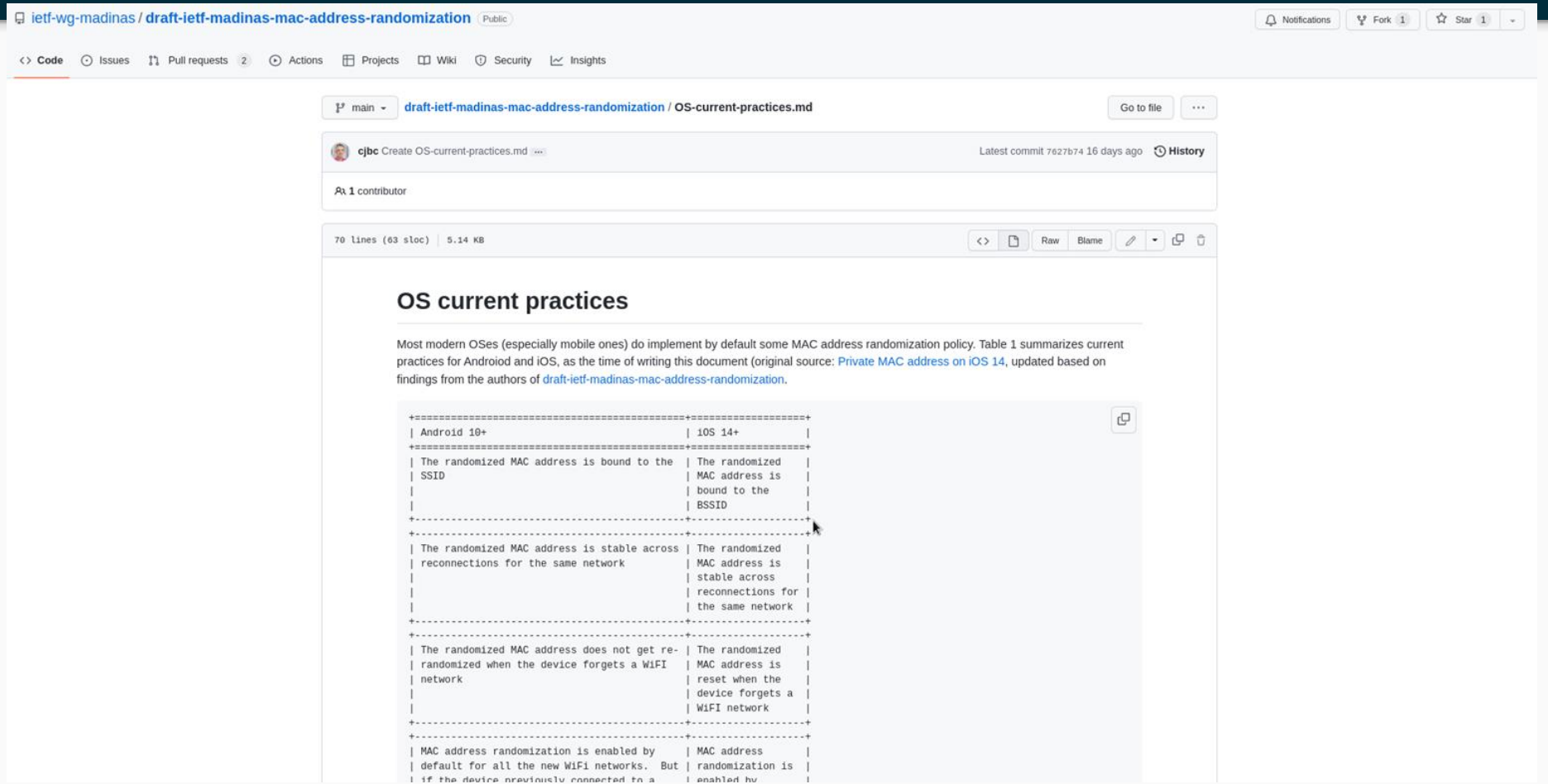
- Privacy, an increasing concern
  - Layer-2 globally unique identifiers (MAC addresses) have been assigned to devices and are transmitted in the clear in, for instance, beacons, probe requests, or after association
  - MAC addresses can easily be intercepted and used to track location or behavior
- 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

IETF

Table of contents

IETF

Table of contents



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.

IETF

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 (PBGM)
  - ## Per-Network Generated MAC address (PNGM)
  - ## Per-Session Generated MAC address (PSGM)
  - ## Per-Period Generated MAC address (PPGM)

IETF

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?