JC. Zuniga
CISCO
CJ. Bernardos, Ed.
UC3M
A. Andersdotter
Safespring AB

20 February 2024

Randomized and Changing MAC Address: A Taxonomy and ~~state~~ State of ~~affairs~~Affairs (2024)

draft-ietf-madinas-mac-address-randomization-11

Abstract

~~Internet privacy has become a major concern over the past few years.~~ Users are becoming more aware that their ~~online~~ activity over the Internet leaves a vast digital footprint, that communications ~~are~~ might not always be properly secured, and that their location and actions can be ~~easily~~ tracked. One of the main factors ~~for the location~~that eases tracking users ~~issue~~ is the wide use of long-lasting, and sometimes persistent, identifiers at various protocols layers. T~~, such~~his document focuses on ~~as~~ MAC addresses.

There have been several initiatives ~~at~~ within the IETF and the IEEE 802 standards committees to overcome some of these privacy issues. This document provides an overview of these activities~~, with the intention to inform the technical community about them, and~~ to help ~~coordinate~~coordinating ~~between present and future~~ standardization activities in these bodies.

Commenté [BMI1]: I would add a mention about the taxonomy.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Internet privacy is becoming a huge concern, as more and more mobile devices are getting directly (e.g., via Wi-Fi) or indirectly (e.g., via a smartphone using Bluetooth) connected to the Internet. This ubiquitous connectivity, together with not very secure protocol stacks and the lack of proper education about privacy make it very easy to track/monitor the location of users and/or eavesdrop their physical and online activities. This is due to many factors, such as the vast digital footprint that users leave on the Internet with or without their consent, for instance sharing information on social networks, cookies used by browsers and servers ~~to provide a better navigation experience~~for various reasons, connectivity logs that allow tracking of a user's Layer~~-~~_2 (L2/MAC) or Layer~~-~~_3 (L3) address, web trackers, etc.; and/or the weak (or even null in some cases) authentication and encryption mechanisms used to secure communications.

This privacy concern affects all layers of the protocol stack, from the lower layers involved in the ~~actual~~ access to the network (e.g., the MAC/Layer~~-~~_2 and Layer~~-~~_3 addresses can be used to obtain the (network) location of a user) to higher layer protocol identifiers and user applications [wifi_internet_privacy]. In particular, IEEE 802 MAC addresses have historically been an easy target for tracking users [wifi_tracking].

Commenté [BMI2]: I guess mobile is mentioned here on purpose as this may "follow the owner" and their track it? Is that the intent of this mention?

Commenté [BMI3]: Not sure what is the purpose of this text?

Commenté [BMI4]: You may provide an example.

Commenté [BMI5]: Fingerprinting is also possible because of how a browzer/app is built. See Panopticlick | About (pbtest.org)

Commenté [BMI6]: The server does not see that MAC address

Commenté [BMI7]: There is also all the "telemetry" out there sent by your device or a neighboring device. Please see https://www.scss.tcd.ie/doug.leith/apple_google.pdf

There have been several initiatives at the IETF and the IEEE 802 standards committees to overcome some of these privacy issues. This document provides an overview of these activities~~, with the intention to inform the community and~~ to help coordinate ~~between present and futures~~ standardization activities within thee bodies.

2. Terminology

The following ~~terms~~ abbreviation ~~are~~ is used in this document:

MAC: Medium Access Control

Commenté [BMI8]: I would delete this section, unless you have more to list here.

3. Background

3.1. MAC ~~A~~address ~~usage~~Usage

Most mobile devices used today are Wi-Fi enabled (i.e., they are equipped with an IEEE 802.11 wireless local area network interface). Wi-Fi interfaces, as any other kind of IEEE 802-based network interface, like Ethernet (i.e., ~~-~~ IEEE 802.3) have a Layer~~-~~ 2 address also referred to as MAC address, which can be seen by anybody who can receive the signal transmitted by the network interface. The format of these addresses is shown in Figure 1.

Commenté [BMI9]: This is trademarked. May be use the WLAN?

Commenté [BMI10]: Add a ref

Commenté [BMI11]: I guess you are referring to the network side, not every node in the Internet. The text may be mis-interpreted.

Commenté [BMI12]: Add the authoritative source


```
           +--------+--------+---------+--------+--------+---------+
           |  Organizationally Unique  |     Network Interface     |
           |     Identifier (OUI)      | Controller (NIC) Specific |
           +--------+--------+---------+--------+--------+---------+
          /          \
         /            \
        /              \         b0 (I/G bit):
       /                \            0: unicast
      /                  \           1: multicast
     /                    \
    /                      \      b1 (U/L bit):
   +--+--+--+--+--+--+--+--+          0: globally unique (OUI enforced)
   |b7|b6|b5|b4|b3|b2|b1|b0|          1: locally administered
   +--+--+--+--+--+--+--+--+
```

Figure 1: IEEE 802 MAC Address Format

MAC addresses can either be universally administered or locally administered. Universally administered and locally administered addresses are distinguished by setting the second-least-significant bit of the most significant byte of the address (the U/L bit).

A universally administered address is uniquely assigned to a device by its manufacturer. Most physical devices are provided with a universally administered address, which is composed of two parts: (i) the Organizationally Unique Identifier (OUI), which are the first three octets in transmission order and identify the organization that issued the identifier, and (ii) Network Interface Controller (NIC) Specific, which are the following three octets, assigned by the organization that manufactured the NIC, in such a way that the resulting MAC address is globally unique.

Locally administered addresses override the burned-in address, and they can either be set-up by the network administrator, or by the Operating System (OS) of the device to which the address pertains. However, as explained in further sections of this document, there are new initiatives at the IEEE 802 and other organizations to specify ways in which these locally administered addresses should be assigned, depending on the use case.

Commenté [BMI13]: Should this section mention that the mac address can be flushed by the user/admin, and that this was used to overcome mac-based filtering in the past?

3.2. MAC A~~a~~ddress R~~r~~andomization

Since universally administered MAC addresses are by definition globally-unique, when a device uses this MAC address to transmit data -especially over the air- it is relatively easy to track this device by simple medium observation. Since a device is usually directly associated to an individual, this poses a privacy concern [link_layer_privacy].

MAC addresses can be easily observed by a third party, such as a passive device listening to communications in the same network. In ~~an~~ a 802.11 network, a station exposes its MAC address in two different situations:

* While actively scanning for available networks, the MAC address is used in the Probe Request frames sent by the device (aka IEEE 802.11 STA).

* Once associated to a given Access Point (AP), the MAC address is used in frame transmission and reception, as one of the addresses used in the address fields of an IEEE 802.11 frame.

One way to overcome this privacy concern is by using randomly generated MAC addresses. As described in the previous section, the IEEE 802 addressing includes one bit to specify if the hardware address is locally or globally administered. This allows generating local addresses without the need of any global coordination mechanism to ensure that the generated address is still unique within the local network. This feature can be used to generate random addresses, which decouple the globally-unique identifier from the device and therefore make it more difficult to track a user device from its MAC/L2 address [enhancing_location_privacy].

Commenté [BMI14]: Which one? Please add a pointer.

Note that there are reports [contact_tracing_paper] of some mobile Operating Systems (OSes) reporting persistently (every 20 minutes or so) on MAC addresses
(among other information), which would defeat MAC address

randomization. While these practices might have changed by now, it is important to highlight that privacy preserving techniques should be conducted considering all layers of the protocol stack.

3.3. Privacy Workshop, Tutorial, and Experiments at IETF and IEEE 802 ~~meetings~~Meetings

As an outcome to the STRINT W3C/IAB Workshop [strint], ~~on July 2014~~ a ~~Tutorial~~ tutorial on "Pervasive Surveillance of the Internet - Designing Privacy into Internet Protocols" was given at the IEEE 802 Plenary meeting in San Diego [privacy_tutorial]. The ~~Tutorial~~ tutorial provided an update on the recent developments regarding Internet privacy, the actions undertaken by ~~that~~ other SDOs such as IETF ~~were taking~~, and guidelines ~~that were being~~ followed when developing new Internet protocol specifications (e.g., ~~-~~ [RFC6973]). The ~~Tutorial~~ tutorial highlighted some p~~P~~rivacy concerns applicable specifically to Link Layer technologies and provided suggestions on how IEEE 802 could help addressing them.

Following the discussions and interest within the IEEE 802 community, on 18 July 2014 the IEEE 802 Executive Committee (EC) created an IEEE 802 EC Privacy Recommendation Study Group (SG) [ieee_privacy_ecsg].

The work and discussions from the group have generated multiple outcomes, such as: 802E PAR: Recommended Practice for Privacy Considerations for IEEE 802 Technologies [IEEE_802E], and the 802c PAR: Standard for Local and Metropolitan Area Networks - Overview and Architecture Amendment - Local Medium Access Control (MAC) Address Usage [IEEE_802c].

In order to test the effects of MAC address randomization, ~~major~~ trials were conducted at the IETF and IEEE 802 meetings between November 2014 and March 2015 - IETF91, IETF92 and IEEE 802 Plenary in Berlin. The purpose of the ~~experiments~~ trials was to evaluate the use of MAC address randomization from two different perspectives: (i) the effect on the connectivity experience of the end-user, also checking if applications and ~~operating systems (~~OSes~~)~~ were affected; and (ii) the potential impact on the network infrastructure itself. Some of the findings were published in [wifi_internet_privacy].

During the ~~experiments~~ trials it was observed that the probability of address duplication in a network with this characteristics is negligible. The ~~experiments~~ trials also ~~showed~~ revealed that other protocol identifiers can be correlated and therefore be used to still track an individual. Hence, effective privacy tools should not work in isolation at a single layer, but they should be coordinated with other privacy features at higher layers.

Since then, MAC randomization has further been implemented by mobile ~~operating systems~~OSes to provide better privacy for mobile phone users when connecting to public wireless networks [privacy_ios], [privacy_windows], [privacy_android].

4. Randomized And Changing MAC Addresses (RCM)~~Recent RCM activities~~ Activities at the IEEE 802

Practical experiences of Randomized ~~And~~ and Changing MAC Addresses (RCM)

Commenté [BMI15]: ?

Commenté [BMI16]: Are you referring to CUI (RFC4372), for example?

If so, I would mention it as an example.

Commenté [BMI17]: I would not be affirmative here I'm not sure yet the practices beyond MAC address allocation were "updated". See https://www.scss.tcd.ie/doug.leith/apple_google.pdf in live devices helped researchers fine-tune their understanding of attacks against randomization mechanisms [when_mac_randomization_fails]. At IEEE 802.11 group these research experiences eventually formed the basis for a specified mechanism introduced in the IEEE 802.11aq in 2018 which randomize MAC addresses that recommends mechanisms to avoid pitfalls [IEEE_802_11_aq].

Commenté [BMI18]: What is a live device?

Commenté [BMI19]: Of what?

More recent developments (as per 2024) include turning on MAC randomization in mobile ~~operating systems~~OSes by default, which has an impact on the ability of network operators to ~~personalize or~~ customize services [rcm_user_experience_csd]. Therefore, follow-on work in the IEEE 802.11 mapped effects of potentially large uptake of randomized MAC identifiers on a number of commonly offered operator services in 2019 [rcm_tig_final_report]. In the summer of 2020 this work emanated in two new standards projects with the purpose of developing mechanisms that do not decrease user privacy ~~and~~ but enable an optimal user experience when the MAC address of a device in an Extended Service Set is randomized or changes [rcm_user_experience_par] and user privacy solutions applicable to IEEE Std 802.11 [rcm_privacy_par].

Commenté [BMI20]: Is there any update from this PARs since then?

IEEE Std 802 [IEEE_802], as of the amendment IEEE 802c-2017 [IEEE_802c], specifies a local MAC address space structure known as the Structured Local Address Plan (SLAP). The SLAP designates a range of Extended Local Identifiers (ELIs) for subassignment within a block of addresses assigned by the IEEE Registration Authority via a Company ID (CID). A range of local MAC addresses is designated for Standard Assigned Identifiers (SAI) to be specified by IEEE 802 standards. Another range of local MAC addresses is designated for Administratively Assigned Identifiers (AAI) subject to assignment by a network administrator.

a mis en forme : Surlignage

"IEEE Std 802E-2020: Recommended Practice for Privacy Considerations for IEEE 802 Technologies" [IEEE_802E] recommends the use of temporary and transient identifiers if there are no compelling reasons for a newly introduced identifier to be permanent. This ~~Recommended~~recommendation ~~Practice~~ is part of the basis for the review of user privacy solutions for IEEE Std 802.11 (aka Wi-Fi) devices as part of the RCM [rcm_privacy_csd] efforts. Annex T of IEEE Std 802.1AEdk-2023 "~~:~~ MAC Privacy Protection" [IEEE802.1AEdk-2023] discusses privacy considerations in bridged networks.

Commenté [BMI21]: Are those "compelling reasons" characterized?

~~Currently~~As per 2024, two task groups in IEEE 802.11 are dealing with issues related to RCM:

* The IEEE 802.11bh task group, looking at mitigating the repercussions that RCM creates on 802.11 networks and related services, and

* The IEEE 802.11bi task group, which ~~will~~ is chartered to define modifications to the IEEE Std 802.11 medium access control (MAC) specification to specify new mechanisms that address and improve user privacy.

5. Recent MAC ~~R~~randomization-related ~~activities~~ Activities at the WBA

At the Wireless Broadband Alliance (WBA), the Testing and Interoperability Work Group has been looking at the issues related to

MAC address randomization and has identified a list of potential impacts of these changes to existing systems and solutions, mainly related to Wi-Fi identification.

As part of this work, 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. A first version of this document has been liaised with the IETF as part of the MAC Address Device Identification for Network and Application Services (MADINAS) activities through the "Wi-Fi Identification In a post MAC Randomization Era v1.0" paper [wba_paper].

6. MAC ~~r~~Randomization in IETF Protocol Standards

[RFC4862] specifies Stateless Address Autoconfiguration (SLAAC) for IPv6, which typically results in hosts configuring one or more "stable" addresses composed of a network prefix advertised by a local router, and an Interface Identifier (IID). [RFC8064] formally updated the original IPv6 IID selection mechanism to avoid generating the IID from the MAC address of the interface (via EUI64), as this potentially allowed for global tracking of a device at L3 from any point on the Internet (note that the prefix part of the address provides meaningful insights of the physical location of the device in general, which together with the MAC address-based IID, made it easier to perform global device tracking).

[RFC8981] identifies and describes the privacy issues associated with embedding MAC stable addressing information into the IPv6 addresses (as part of the IID). It describes an extension to IPv6 Stateless Address Autoconfiguration that causes hosts to generate temporary addresses with randomized interface identifiers for each prefix advertised with autoconfiguration enabled. Changing addresses over time limits the window of time during which eavesdroppers and other information collectors may trivially perform address-based network-activity correlation when the same address is employed for multiple transactions by the same host. Additionally, it reduces the window of exposure of a host as being accessible via an address that becomes revealed as a result of active communication. These temporary addresses are meant to be used for a short period of time (hours to days) and would then be deprecated. Deprecated addresses can continue to be used for already established connections, but are not used to initiate new connections. New temporary addresses are generated periodically to replace temporary addresses that expire. In order to do so, a node produces a sequence of temporary global scope addresses from a sequence of interface identifiers that appear to be random in the sense that it is difficult for an outside observer to predict a future address (or identifier) based on a current one, and it is difficult to determine previous addresses (or identifiers) knowing only the present one. The main problem with the temporary addresses is that they should not be used by applications that listen for incoming connections (as these are supposed to be waiting on permanent/well-known identifiers). Besides, if a node changes network and comes back to a previously visited one, the temporary addresses that the node would use will be different, and this might be an issue in certain networks where addresses are used for operational purposes (e.g., filtering or authentication). [RFC7217], summarized next, partially addresses the problems aforementioned.

[RFC7217] describes a method to generate Interface Identifiers that are stable for each network interface within each subnet, but that change as a host moves from one network to another. This method enables keeping the "stability" properties of the Interface Identifiers specified in [RFC4291], while still mitigating address-scanning attacks and preventing correlation of the activities of a host as it moves from one network to another. The method defined to generate the IPv6 IID is based on computing a hash function which takes as input information that is stable and associated to the interface (e.g., a local interface identifier), stable information associated to the visited network (e.g., IEEE 802.11 SSID), the IPv6 prefix, and a secret key, plus some other additional information. This basically ensures that a different IID is generated when any of the input fields changes (such as the network or the prefix), but that the IID is the same within each subnet.

Currently, [RFC8064] recommends nodes to implement [RFC7217] as the default scheme for generating stable IPv6 addresses with SLAAC, to mitigate the privacy threats posed by the use of MAC-derived IIDs.

In addition to the former documents, [RFC8947] proposes an extension to DHCPv6 that allows a scalable approach to link-layer address assignments where preassigned link-layer address assignments (such as by a manufacturer) are not possible or unnecessary. [RFC8948] proposes extensions to DHCPv6 protocols to enable a DHCPv6 client or a DHCPv6 relay to indicate a preferred SLAP quadrant to the server, so that the server may allocate MAC addresses in the quadrant requested by the relay or client.

Not only MAC and IP addresses can be used for tracking purposes. Some DHCP options carry unique identifiers. These identifiers can enable device tracking even if the device administrator takes care of randomizing other potential identifications like link-layer addresses or IPv6 addresses. [RFC7844] introduces anonymity profiles, designed for clients that wish to remain anonymous to the visited network. The profiles provide guidelines on the composition of DHCP or DHCPv6 messages, designed to minimize disclosure of identifying information. [RFC7844] also indicates that the link-layer address, IP address, and DHCP identifier shall evolve in synchrony.

Commenté [BMI22]: Should RFC 9414, 9415, 9416 be listed in this section as well?

7. A ~~taxonomy~~ Taxonomy of MAC ~~address~~ Address ~~selection~~ Selection ~~policies~~Policies

Commenté [BMI23]: I would add a mention about this to the abstract. For me this is one of the key contributions of this draft.

This section documents different policies for MAC address selection. ~~Note that some~~Some OSes might use combination of multiple of these policies.

Note about the used naming convention: the "M" in MAC is included in the acronym, but not the "A" from address. This allows one to talk about a PVOM Address, or PNGM Address.

The names are all in the form for per-period-of-time-selection.

7.1. Per-Vendor OUI MAC ~~A~~address (PVOM)

This form of MAC address selection is the historical default.

The vendor obtains an Organizationally Unique Identifier (OUI) from the IEEE. This has been a 24-bit prefix (including two upper bits which are set specifically) that is assigned to the vendor. The vendor generates a unique 24-bit value for the lower 24-bits, forming the 48-bit MAC address. It has not been unusual for the 24-bit value to be taken as an incrementing counter, assigned at the factory, and burnt into non-volatile storage.

Note that 802.15.4 use 64-bit MAC addresses, and the IEEE assigns 32-bit prefixes. The IEEE has indicated that there may be a future Ethernet specification using 64-bit MAC addresses.

7.2. Per-Device Generated MAC ~~address~~ 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.

7.3. Per-Boot Generated MAC ~~address~~ 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).

7.4. Per-Network Generated MAC ~~adress~~ Adress (PNGM)

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

Commenté [BMI24]: As the same @ is used when reattaching to the same network.

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.

7.5. Per-Period Generated MAC ~~address~~ 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. TBD: it is unclear if any TLS session-resumption ticket (used by EAP-TLS) can or should be retained across a change of the MAC address.

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.

7.6. Per-Session Generated MAC A~~a~~ddress (PSGM)

This form of MAC address is generated on a per session basis. Like PNGM, it is used primarily with WiFi (802.11).

Since the address changes only when a new session is established, there is no disconnection/reconnection involved.

8. OS current practices

Most modern OSes (especially mobile ones) do implement by default some MAC address randomization policy. Since the mechanism and policies OSes implement can evolve with time, the content is now hosted at https://github.com/ietf-wg-madinas/draft-ietf-madinas-mac-address-randomization/blob/main/OS-current-practices.md. For completeness, a snapshop of the content at the time of publication of this document is included below.

Table 1 summarizes current practices for Androi~~o~~d and iOS, as the time of writing this document (original source: https://www.fing.com/news/private-mac-address-on-ios-14, updated based on findings from the authors).

Commenté [BMI25]: I would remove the tables and keep only the github pointer.

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

Table 1: Android and iOS MAC address randomization practices

In September 2021, we have performed some additional tests to evaluate how most widely used OSes behave regarding MAC address randomization. Table 2 summarizes our findings, where show on different rows whether the OS performs address randomization per network, per new connection, daily, supports configuration per SSID, supports address randomization for scanning, and whether it does that by default.

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

Table 2: Observed behavior from different OS (as of September 2022)

According to [privacy_android], starting in Android 12, Android uses non-persistent randomization in the following situations: (i) a network suggestion app specifies that non-persistant 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).

9. IANA Considerations

N/A.

10. Security Considerations

Privacy considerations regarding tracking the location of a user through the MAC address of this device are discussed throughout this document. Given the informational nature of this document, no protocols/solutions are specified, but current state of affairs is documented.

Any future specification in this area would have to look into security and privacy aspects, such as, but not limited to: i) mitigating the problem of location privacy while minimizing the impact on upper layers of the protocol stack; ii) providing means to network operators to authenticate devices and authorize network access despite the MAC addresses changing following some pattern; and, iii) provide means for the device not to use MAC addresses it is not authorized to use or that are currently in use.

A major conclusion of the work in IEEE Std 802E concerned the difficulty of defending privacy against adversaries of any sophistication. In particular it has been shown that individuals can be successfully tracked by fingerprinting using aspects of their communication other than MAC Addresses or other permanent identifiers. Machine learning techniques facilitate fingerprinting without the adversary needing to understand the technical reasons for the correlation.

11. Acknowledgments

Authors would like to thank Guillermo Sanchez Illan for the extensive tests performed on different OSes to analyze their behavior regarding address randomization.

Authors would like to thank Jerome Henry, Hai Shalom, Stephen Farrel, Alan DeKok, Mathieu Cunche, Johanna Ansohn McDougall, Peter Yee, Bob Hinden, Behcet Sarikaya and David Farmer for their review and comments on previous versions of this document. Authors would also like to thank Michael Richardson for his contributions on the taxonomy section. Finally, authors would also like to thank the IEEE 802.1 Working Group for its review and comments.

12. Informative References

[contact_tracing_paper]
Leith, D. J. and S. Farrell, "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", IEEE INFOCOM 2021~~.~~, July 2020.

[enhancing_location_privacy]
Gruteser, M. and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis", Mobile Networks and Applications, vol. 10, no. 3, pp. 315-325~~.~~, 2005.

[IEEE802.1AEdk-2023]
IEEE 802.1, "IEEE Std 802.1AEdk-2023: IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security - Amendment 4: MAC Privacy protection", 2023.

[IEEE_802] IEEE 802, "IEEE Std 802 - IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", IEEE 802~~.~~, 2014.

[IEEE_802c]
IEEE 802.1 WG - 802 LAN/MAN architecture, "IEEE 802c-2017 - IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture--Amendment 2: Local Medium Access Control (MAC) Address Usage", IEEE 802c~~.~~, 2017.

[IEEE_802E]
IEEE 802.1 WG - 802 LAN/MAN architecture, "IEEE 802E-2020 - IEEE Recommended Practice for Privacy Considerations for IEEE 802 Technologies", IEEE 802E~~.~~, 2020.

[IEEE_802_11_aq]
IEEE 802.11 WG - Wireless LAN Working Group, "IEEE 802.11aq-2018 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Preassociation Discovery", IEEE 802.11~~.~~, 2018.

[ieee_privacy_ecsg]
IEEE 802 Privacy EC SG, "IEEE 802 EC Privacy

Recommendation Study Group",
<http://www.ieee802.org/PrivRecsg/>.

[link_layer_privacy]
O'Hanlon, P., Wright, J., and I. Brown, "Privacy at the link layer", Contribution at W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)~~.~~, February 2014.

[privacy_android]
Android Open Source Project, "MAC Randomization Behavior", <https://source.android.com/devices/tech/connect/wifi-mac-randomization-behavior>.

[privacy_ios]
Apple, "Use private Wi-Fi addresses in iOS 14, iPadOS 14, and watchOS 7", <https://support.apple.com/en-us/HT211227>.

[privacy_tutorial]
Cooper, A., Hardie, T., Zuniga, JC., Chen, L., and P. O'Hanlon, "Tutorial on Pervasive Surveillance of the Internet - Designing Privacy into Internet Protocols", <https://mentor.ieee.org/802-ec/dcn/14/ec-14-0043-01-00EC-internet-privacy-tutorial.pdf>.

[privacy_windows]
Microsoft, "Windows: How to use random hardware addresses", <https://support.microsoft.com/en-us/windows/how-to-use-random-hardware-addresses-ac58de34-35fc-31ff-c650-823fc48eb1bc>.

[rcm_privacy_csd]
IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group CSD on user experience mechanisms", doc.:IEEE 802.11-20/1346r1~~.~~, 2020.

[rcm_privacy_par]
IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group PAR on privacy mechanisms", doc.:IEEE 802.11-19/854r7~~.~~, 2020.

[rcm_tig_final_report]
IEEE 802.11 WG RCM TIG, "IEEE 802.11 Randomized And Changing MAC Addresses Topic Interest Group Report", doc.:IEEE 802.11-19/1442r9~~.~~, 2019.

[rcm_user_experience_csd]
IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group CSD on user experience mechanisms", doc.:IEEE 802.11-20/1117r3~~.~~, 2020.

[rcm_user_experience_par]
IEEE 802.11 WG RCM SG, "IEEE 802.11 Randomized And Changing MAC Addresses Study Group PAR on user experience mechanisms", doc.:IEEE 802.11-20/742r5~~.~~, 2020.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing

Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <https://www.rfc-editor.org/info/rfc7844>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8947] Volz, B., Mrugalski, T., and C. Bernardos, "Link-Layer Address Assignment Mechanism for DHCPv6", RFC 8947, DOI 10.17487/RFC8947, December 2020, <https://www.rfc-editor.org/info/rfc8947>.

[RFC8948] Bernardos, CJ. and A. Mourad, "Structured Local Address Plan (SLAP) Quadrant Selection Option for DHCPv6", RFC 8948, DOI 10.17487/RFC8948, December 2020, <https://www.rfc-editor.org/info/rfc8948>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[strint] W3C/IAB, "A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)", <https://www.w3.org/2014/strint/>.

[wba_paper]
Alliance, W. B., "Wi-Fi Identification Scope for Liasing - In a post MAC Randomization Era", doc.:WBA Wi-Fi ID Intro: Post MAC Randomization Era v1.0 - IETF liaison~~.~~, March 2020.

[when_mac_randomization_fails]
Martin, J., Mayberry, T., Donahue, C., Foppe, L., Brown, L., Riggins, C., Rye, E.C., and D. Brown, "A Study of MAC Address Randomization in Mobile Devices and When it Fails", arXiv:1703.02874v2 [cs.CR]~~.~~, 2017.

[wifi_internet_privacy]
Bernardos, CJ., Zúñiga, JC., and P. O'Hanlon, "Wi-Fi Internet Connectivity and Privacy: Hiding your tracks on the wireless Internet", Standards for Communications and Networking (CSCN), 2015 IEEE Conference on~~ ,~~, October 2015.

[wifi_tracking]
The Independent, "London's bins are tracking your smartphone", <https://www.independent.co.uk/life-style/gadgets-and-tech/news/updated-london-s-bins-are-tracking-your-smartphone-8754924.html>.

Authors' Addresses

Juan Carlos Zuniga
CISCO
Montreal QC
Canada
Email: juzuniga@cisco.com

Carlos J. Bernardos (editor)
Universidad Carlos III de Madrid
Av. Universidad, 30
28911 Leganes, Madrid
Spain
Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Amelia Andersdotter
Safespring AB
Email: amelia.ietf@andersdotter.cc