MAC address randomization
draft-zuniga-mac-address-randomization-01

Abstract

   Internet privacy has become a major concern over the past few years.
   Users are becoming more aware that their online activity leaves a
   vast digital footprint, that communications are not always properly
   secured, and that their location and actions can be easily tracked.
   One of the main factors for the location tracking issue is the wide
   use of long-lasting identifiers, such as MAC addresses.

   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 technical community about them, and help coordinate
   between present and futures standardization activities.

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 cellular or 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, for instance sharing information on social networks,
   cookies used by browsers and servers to provide a better navigation

experience, 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
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].

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 help coordinate between present and
futures standardization activities.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

The following terms are used in this document:

   MAC: Medium Access Control

3. Background

3.1. MAC address 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.

Figure 1: IEEE 802 MAC Address Format (TBD)

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.

3.2. MAC address randomization

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 802.11 network, a station exposes its MAC address in two different
situations:

o 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).

o 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].

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

As an outcome to the STRINT W3C/IAB Workshop [strint], on July 2014 a
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 provided an
update on the recent developments regarding Internet privacy, the
actions 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 highlighted some
Privacy 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 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 (OSs) 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 it was observed that the probability of
address duplication in a network with this characteristics is
negligible. The experiments also showed 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 to provide better privacy for mobile phone users

when connecting to public wireless networks [privacy_ios],
[privacy_windows], [privacy_android].

4. **Recent RCM activities at the IEEE 802**

Practical experiences of Randomized And Changing MAC Addresses (RCM)
in live devices helped researchers fine-tune their understanding of
attacks against randomization mechanisms
[when_mac_randomization_fails]. At IEEE 802.11 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].

More recent developments include turning on MAC randomization in
mobile operating systems 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 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].

The IEEE 802.1 working group has also published a specification that
defines a local MAC address space structure, known as the Structured
Local Address Plan (SLAP). This structure designates a range of
local MAC addresses for protocols using a Company ID (CID) assigned
by the IEEE Registration Authority. Another range of local MAC
addresses is designated for assignment by administrators. The
specification recommends a range of local MAC addresses for use by
IEEE 802 protocols [IEEE_802c].

Work within the IEEE 802.1 Security task group on privacy
recommendations for all IEEE 802 network technologies has also looked
into general recommendations on identifiers, reaching the conclusion
that temporary and transient identifiers are preferably in network
technology design if there are no compelling reasons of service
quality for a newly introduced identifier to be permanent. This work
has been specified in the recently published IEEE P802E: Recommended
Practice for Privacy Considerations for IEEE 802 Technologies
[IEEE_802E]. The IEEE P802E specification will form part of the
basis for the review of user privacy solutions applicable to IEEE Std
802.11 (aka Wi-Fi) devices as part of the RCM [rcm_privacy_csd]
efforts.

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

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

o The IEEE 802.11bi task group, which will 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 randomization-related 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
realted 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 randomization-related activities at the IETF

Several IP address assignment mechanisms such as the IPv6 stateless
autoconfiguration techniques (SLAAC) [RFC4862] generate the Interface
Identifier (IID) of the address from its MAC address (via EUI64),
which then becomes visible to all IPv6 communication peers. This
potentially allows for global tracking of a device at L3 from any
point on the Internet. Besides, 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, makes it
easier to perform global device tracking.

There are some solutions that might mitigate this privacy threat,
such as the use of temporary addresses [RFC4191], the use of opaque
IIDs [RFC7217], [I-D.gont-6man-deprecate-eui64-based-addresses].
Next, we briefly describe how these solutions work.

[RFC4191] identifies and describes the privacy issues associated with
embedding MAC stable addressing information into the IPv6 addresses
(as part of the IID) and describes some mechanisms to mitigate the
associated problems. The specification is meant for IPv6 nodes that

auto-configure IPv6 addresses based on the MAC address (EUI-64
mechanism). It defines how to create additional addresses (generally
known as "temporary addresses") based on a random interface
identifier for the purpose of initiating outgoing sessions. These
"random" or 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] defines a method for generating IPv6 IIDs to be used with
IPv6 Stateless Address Autoconfiguration (SLAAC), such that an IPv6
address configured using this method is stable within each subnet,
but the corresponding IID changes when the host moves from one
network to another. This method is meant to be an alternative to
generating Interface Identifiers based on MAC addresses, such that
the benefits of stable addresses can be achieved without sacrificing
the security and privacy of users. 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., MAC address or 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.

In addition to the former documents, [I-D.ietf-dhc-mac-assign]
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. [I-D.ietf-dhc-slap-quadrant] 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.

Lately, the MAC Address Device Identification for Network and Application Services (MADINAS) IETF BoF has discussed the need to examine the effect of RCM schemes on network and application services in several scenarios identified as relevant.

7. 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: https://www.fing.com/news/private-mac-address-on-ios-14, updated based on findings from the authors).

```
+-------------------------------+-------------------------------+
| Android 10+                   | iOS 14+                       |
+-------------------------------+-------------------------------+
| The randomized MAC address is | The randomized MAC address is |
| bound to the SSID             | bound to the BSSID            |
|                               |                               |
| The randomized MAC address is | The randomized MAC address is |
| stable across reconnections for | stable across reconnections for |
| the same network              | the same network              |
|                               |                               |
| The randomized MAC address is | The randomized MAC address is |
| reset when the device forgets a | reset when the device forgets a |
| WiFI network                  | WiFI network                  |
|                               |                               |
| MAC address randomization is  | MAC address randomization is  |
| enabled by default for all the | enabled by default for all the |
| new WiFi networks. But if the | new WiFi networks             |
| device previously connected to |                               |
| a WiFi network identifying    |                               |
| itself with the real MAC      |                               |
| address, no randomized MAC    |                               |
| address will be used (unless  |                               |
| manually enabled)             |                               |
+-------------------------------+-------------------------------+
```

        Table 1: Android and iOS MAC address randomization practices

8. IANA Considerations

   N/A.

9. Security Considerations

   TBD.

10. Acknowledgments

   TBD.

11. References

11.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

11.2. Informative References

[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.

[I-D.gont-6man-deprecate-eui64-based-addresses]
          Gont, F., Cooper, A., Thaler, D., and W. Liu, "Deprecating
          EUI-64 Based IPv6 Addresses", draft-gont-6man-deprecate-
          eui64-based-addresses-00 (work in progress), October 2013.

[I-D.ietf-dhc-mac-assign]
          Volz, B., Mrugalski, T., and C. J. Bernardos, "Link-Layer
          Address Assignment Mechanism for DHCPv6", draft-ietf-dhc-
          mac-assign-09 (work in progress), September 2020.

[I-D.ietf-dhc-slap-quadrant]
          Bernardos, C. J. and A. Mourad, "Structured Local Address
          Plan (SLAP) Quadrant Selection Option for DHCPv6", draft-
          ietf-dhc-slap-quadrant-12 (work in progress), October
          2020.

[IEEE_802_11_aq]
          Group, 8. W. -. W. L. W., "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_802c]
          architecture, 8. W. -. 8. L., "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]
          architecture, 8. W. -. 8. L., "IEEE 802E-2020 - IEEE
          Recommended Practice for Privacy Considerations for IEEE
          802 Technologies", IEEE 802E , 2020.

[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]
             Google/Open Handset Alliance, "Android Privacy: MAC
             Randomization",
             <https://source.android.com/devices/tech/connect/wifi-mac-
             randomization>.

   [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]
             SG, 8. W. R., "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]
             SG, 8. W. R., "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]
             TIG, 8. W. R., "IEEE 802.11 Randomized And Changing MAC
             Addresses Topic Interest Group Report", doc.:IEEE
             802.11-19/1442r9 , 2019.

[rcm_user_experience_csd]
          SG, 8. W. R., "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]
          SG, 8. W. R., "IEEE 802.11 Randomized And Changing MAC
          Addresses Study Group PAR on user experience mechanisms",
          doc.:IEEE 802.11-20/742r5 , 2020.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
          More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191,
          November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[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>.

[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., 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., Zuniga, 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
   SIGFOX
   Montreal QC
   Canada

   Email: j.c.zuniga@ieee.org

   Carlos J. Bernardos
   Universidad Carlos III de Madrid
   Av. Universidad, 30
   Leganes, Madrid 28911
   Spain

   Phone: +34 91624 6236
   Email: cjbc@it.uc3m.es
   URI: http://www.it.uc3m.es/cjbc/

   Amelia Andersdotter
   CENTR
   Belliardstraat 20 (6th floor)
   Brussels 1040
   Belgium

   Email: amelia@centr.org
   URI: https://www.centr.org