19 March 2024

IETF MADINAS WG

MAC Address Device Identification for Network and Application Services

This session is being recorded

Chairs:
Juan Carlos Zúñiga – Cisco
Carlos J. Bernardos – UC3M

IETF

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Note Really Well

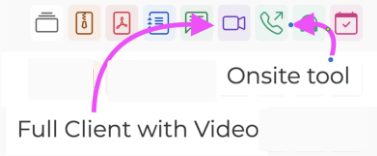
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

This session is being recorded

IETF 119 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Resources for IETF 119 Brisbane

- Agenda
  datatracker.ietf.org/meeting/119/materials/agenda-119-madinas
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

- 17:30: Welcome, Agenda Review and Status Update (WG Chairs)
- 17:35: MAC Address Randomization current state-of-affairs (Carlos J. Bernardos)
- 17:40: Use cases and Problem statement (Jerome Henry)
- 17:50: Liaison from WBA and OpenRoaming update (WG Chairs)
- 17:55: Next Steps (WG Chairs w/AD Support)

WG Status Update

- WG items
  - MAC Address Randomization current state-of-affairs
    - Ready for publication?
  - Use Cases and Identity Requirements
    - WGLC?
  - Best Current Practices handling RCM
    - To be replaced by Informational Annex in Use Cases doc?

- Liaison Statement to IETF MADINAS and RADEXT WGs
  - https://datatracker.ietf.org/liaison/1899/

WBA Liaison - Background

- WBA has recently liaised with both MADINAS and RADEXT Working Groups, first introducing the OpenRoaming federation (https://datatracker.ietf.org/liaison/1848/) as well as more recently around the topic of privacy leakage across the federation (https://datatracker.ietf.org/liaison/1862/).
- Subsequently at IETF118, WBA members participated in the OpenRoaming hackathon aimed at analyzing the possible leakage of privacy information by a variety of OpenRoaming identity providers for a variety of different OpenRoaming access network provider use-cases. Results presented confirmed that certain OpenRoaming identity providers were configuring attributes in the RADIUS Access-Accept message that could weaken the privacy of end-users (https://datatracker.ietf.org/meeting/118/materials/slides-118-madinas-hackathon-openroaming-update-00).

WBA Liaison - Updates

- WBA would like to share with MADINAS and RADEXT working groups that it has now updated its WRIX and OpenRoaming specifications to include normative text regarding end-user privacy, aimed at preventing the unintentional weakening of end-user privacy by the use of correlation identifiers in RADIUS Access-Accept messages.

WBA Liaison – Recommendation (1/2)

- WBA now recommends that the default identity provider policy should ensure that any correlation identifiers in the RADIUS Access-Accept message, such as Class attribute (#25) and/or Chargeable-User-Identity attribute (#89), are unique for each combination of end-user and access network provider and that the keys and/or initialization vectors used in creating such correlation identifiers should be refreshed at least every 48 hours, but not more frequently than every two hours.
- This two hour limit is designed to permit the access network provider to perform autonomous troubleshooting of connectivity issues from authentic users/devices that are repeatedly re-initiating connectivity to the access provider's network and/or permit the access provider to identify a new session originated by an authentic user/device that has previously violated the OpenRoaming end-user terms and conditions.

WBA Liaison – Recommendation (2/2) + Next Steps

- In contrast to this default policy, WBA WRIX specifications describe scenarios where the 48 hour limit is required to be extended, for example when the identity provider supports settled service and requires the correlation identifier to be stable over an entire billing period.
- WBA has worked with the authors of OpenRoaming I-D to update the draft to reflect these recent changes (https://www.ietf.org/archive/id/draft-tomas-openroaming-02.html <https://www.ietf.org/archive/id/draft-tomas-openroaming-02.html>).
- WBA plans to communicate these changes to all OpenRoaming identity providers to ensure they are aware of the updated recommendations.
- Request
  - WBA would welcome the opportunity to present the OpenRoaming I-D to the RADEXT WG at IETF 119.