RCM Work at IEEE

Jerome Henry

March 2023

v 01

IEEE 802.11bh

- An RCM TIG/SG was formed in 2019 by IEEE 802.11 WG, concluded in 2020, and resulted in the formation of 2 groups:
- ***802.11bh: Enhanced service with randomized MAC addresses***
  - *The goal: given RCM, are there services that break with current 802.11?*
    - *Note that the goal is not to fix the entire world, not to 'encourage' or 'discourage' RCM, not to address privacy aspects (although the proposed solution should not degrade privacy in 802.11)*
  - *Some 802.11-centric services that break with RCM:*
    - *Identify a STA when troubleshooting, spot a STA connecting to a secure then to an insecure network, identifying a returning STA (home automation, Guest portals, etc.)*

IEEE 802.11bh Progress

- *Group has agreed on a first scheme (AP provides an identifier to a STA – the STA can indicate this identifier to this or another AP to be identified again)*
- *Debate is ongoing about pre-association recognition*
  - *The scheme is useful in some scenario (e.g., band steering, resource discovery) but presents privacy challenges if misused*
- *The possibility of also using a MAC as an identifier is also discussed*
  - *There are implementation challenges if the MAC needs to be used ‘on-the-fly’*
- *Group is delayed, current target is mid 2024 (from initial mid 2023)*

IEEE 802.11bi

- An RCM TIG/SG was formed in 2019 by IEEE 802.11 WG, concluded in 2020, and resulted in the formation of 2 groups:
- ***802.11bi: Enhanced service with Data Privacy Protection***
  - *The goal: can 802.11 be enhanced to offer better privacy?*
    - *Note that the goal is not to look at the consequences of RCM, although it is understood that RCM has a positive impact on privacy for personal devices*
  - *The group is examining which 802.11 elements have an impact on privacy and how they could be better protected*

IEEE 802.11bi Progress

- 50+ requirements have been identified so far, very 802.11-centric, e.g.:
  - Obfuscate 802.11 key identifiers in reassociations, reduce fingerprint exposure in probe messages and others, allow in-association MAC rotation, obfuscate the MAC addresses in some exchanges, etc.
  - A double goal was identified: protect the STA; protect both the AP and the STA
    - New mechanisms will be required, that may not be compatible with existing Wi-Fi modes
  - *Contributors have started proposing text toward a first draft*
  - *The group will publish enhancements to the IEEE 802.11 Standard*
  - *Group work is expected to be longer than 802.11bh (publication by mid-2026)*

References

- https://www.ieee802.org/11/Reports/802.11_Timelines.htm
- https://mentor.ieee.org/802.11/documents