RCM Work at IEEE

Jerome Henry

March 2022

v 01

IEEE 802E

- Following IETF work in 2013-2015 on privacy, IEEE 802 (under the umbrella of the IEEE 802.1 Security Workgroup) published a *Recommended Practice for Privacy Considerations for IEEE 802 Technologies*
  - *https://standards.ieee.org/standard/802E-2020.html*
- *RCM is not directly recommended, however:*
- a) Temporary identifiers should be used or at least permitted, especially for the use of short-lived services such as network probes.
- b) Temporary identifiers should not persist across different stages of the communication process and should be restricted to specific protocol exchanges. (clause 8)

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

- *9 solutions proposed so far, in 3 general directions:*
  - *STA generates a Layer 2 ID, somehow passes it to the AP after association (secure tunnel), then foretells the AP of its next ID/MAC*
  - *AP generates a Layer 2 ID for the STA, passes it to the STA after association (secure tunnel) -> STA signals that ID at next association (then AP generates a new one)*
  - *AP and STA exchange keys allowing common computation of an ID or a MAC, so AP recognizes the STA at next association*
- *Group is working on prioritizing among proposals, next step will be to start developing 802.11 text*
- *Group work is expected to be rather short (publication by 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

- Close to 20 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.

  - *The group will publish enhancements to the IEEE 802.11 Standard*
  - *Group work is expected to be longer than 802.11bh (publication by mid-2025)*

References

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