MADINAS

RCM Informational Problem Statement Framework

https://datatracker.ietf.org/doc/draft-henry-madinas-framework/

Jerome Henry, Yiu Lee

November 2021

v 01

Draft Scope

- Analyze Use Cases where RCM* affects Network Services
- Analyze Use Cases where RCM affects User Experiences
- List of Requirements

https://datatracker.ietf.org/doc/draft-henry-madinas-framework/

*RCM: Randomized and Changing MAC addresses

Draft Updates – Use Cases 1/2

Definition of use cases for RCM, by triaging contributing elements:

- User vs. Device ; Personal vs. Managed devices
- Who are “they”? Actors involved in network operations
    - Network functional entities (802.11 entities [APs*, WLCs**], switches, routers, 802.1X/DHCP services and more)
    - Human-related entities (OTA observers, wireless network operators, network access providers, OTWi/OTWe observers)

*WiFi access points, ** Wireless LAN Controllers

OTA: over the air, OTW: over the wire (i=internal, e=external)

Draft Updates – Use Cases 2/2

Definition of use cases for RCM, by triaging contributing elements (cont.):

- “Trust” variable (full trust, vs. selective trust, vs. zero trust)
- Environments (individual residential settings, managed residential settings, public guest networks, enterprise, with BYOD or MDM)
- Network entities that track the MAC today (L2 infra, 802.1X/DHCP services, routers, policy engines)
- Current assumptions on RCM

Draft Updates – Requirements

- The network must not make any assumption about client MAC address persistence.
- MAC address change must happen while allowing for service continuity.
- If a service is interrupted during the RCM process, there must be a formal mechanism for the client and the network to exchange about the interruption.
- During duration of the services, the device should not change the identity (or interruptions would occur)

Draft Updates – Possible Steps

- Survey the current standards that use MAC address as a device identifier in the protocol. Make recommendation to the working groups to remove the dependency.
- Identify a secure mechanism to authenticate and exchange network identity to the device.
- Identify a secure mechanism to inform the device about the type of network the device is connecting to (e.g. public Wi-Fi, enterprise, home), allowing the user to select the device identity (or identities) accordingly (e.g. ‘real id or random?’)
- Identify a secure mechanism for the network to request device identity. Upon successful authentication, the network may provide the device a temporary network-based marker to use the network services.
- Identify a secure mechanism for the device to notify the network prior to updating the MAC address.
- Examine the case of IoT.

Draft History

- v00 in March 2021, v01 revision in April, v02 revision in May after MADINAS presentations and exchanges, v03 in October after multiple feedback
- Since October additional feedback on editorial and technical items
- *feedback and additional input are welcome and encouraged*

Elements of Discussion From Recent Comments

- Full Trust and Residential Settings (Section 3.3):
  - *Draft envisions scenarios where fill trust is possible(see 3.3 1 for full trust, and environments type A)*
  - *Comments keep coming that you can’t trust your family, or your neighbors, or you may suddenly call “home” an RB&B*
  - *Are there full trust environments, i.e. environments where full trust IN GENERAL can be assumed?*

Elements of Discussion From Recent Comments

- Race Conditions (Section 3.4):
  - *802.11aq (2018) forbids changing the MAC during association : "The non-AP STA connecting to an infrastructure BSS shall retain a single MAC address for the duration of its connection across an ESS."*
  - *Section 3.4 envisions that RCM can happen at rather fast pace (e.g. every few minutes), section 3.4 does not qualify how the change would happen (with new association or within a single association, as 802.11bh/bi are envisioning both cases)*
  - *Should we keep this assumption, or limit the draft to what has been observed in the past (slow rotations), with the risk of getting an obsolete draft soon? Or should we clarify what is observed (point to draft Zunica?)*