IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identifiable Random MAC, IRM  Advantages  and  Use Cases from 21/0332 Issues Tracking Document | | | | |
| Date: 2021-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Advantages of IRM and Analysis of IRM and Use Cases

Rev 1 – Added brief description of IRM

1. **BRIEF DESCRIPTION OF IDENTIFIABLE RANDOM MAC ADDRESS (IRMA)**

* STA produces a random MAC address from 46 random bits, plus the “01” local admin.
  + a perfectly normal random MAC,
  + Termed “IRMA”.
  + The STA chooses a new random MAC every time, so the IRMA, the TA, changes every time.
* STA then calculates a 128-bit hash, the IRM Hash, using a 128 bit private key, **IRMK**,
  + IRM Hash = SHA-256/128(IRMA, IRMK) .
  + As the IRMA (i.e. the TA) changes, then so does the IRM Hash.  Hence, impossible to know if this is the same STA as before as it has no resemblance at all to previous associations.
* STA then sends Association Request with an IRM Element that includes the IRM Hash, and an indication to the AP if the STA is “Known” or “Unknown” i.e. whether the AP has or has not the private key IRMK.
  + STA can also indicate “private”, and omit the IRM Hash.
  + MAC address is then NOT an IRMA.
* Once associated, if STA is “Unknown”, AP sends IRMK Request Action frame and STA responds with the IRMK.  The IRMK then is an identity for the STA.
* If STA is “Known”, AP can search through its store of IRMKs to find the one that together with the IRMA (i.e. the TA from the STA) produces the IRM Hash that is in the IRM element.
* STA can change IRMK at any time.
  + AP will still know it is the same STA.
* STA can add the IRMK Check field to the IRM element,
  + AP can down-select IRMKs if it has lots of IRMKs to search through.
  + AP can request the IRMK Check to down select IRMKs

1. **ADVANTAGES OF IRM (over present RCM)**

* **A different Random MAC can be used even when returning to same ESS – more privacy!**
  + Even though STA indicates “Known”, No way a 3rd party can know if same STA as previously (unlike present 11aq scheme “same MAC address for same AP”)
  + MAC address and IRM Hash field values change every time. The last associated IRMK stays constant at the AP.
* **An IRM STA can still choose to use “private” random MAC**
  + If no IRM Hash field, then private MAC address in use.
  + Staisfies the “opt-in” requirement.
* **STA can change IRMK at any time**
  + Can change when associated.
  + No way 3rd party can know if IRMK changed. Hence even if brute force to find IRMK, if changed, impossible to know if same STA reassociates.
    - Huge deterrent to attack
  + AP still knows that it is STA X even though IRMK has changed.
* **AP can restrict its stored list if necessary and request a new IRMK if “No IRMK found”**
  + STA can provide old or new IRMK
  + STA could see this as a threat.
  + However, “IRMK Check” allows AP to keep a large store
* **IRMK Check allows AP to keep long IRMK lists**.
  + STA could include if itconsiders AP is a ‘busy AP’ likely to have many IRMKs
  + AP can request ‘check’ if it wants to down-select IRMKs
* **STA can be identified pre-association** 
  + AP can check stored IRMKs as soon as Association Request received OR wait for association
  + STA can send IRMK-ANQP element
* **No reference to any ‘real’ address or real ID**
  + AP can store IRMK against other STA identifier (higher layer), or simply knows it is the same STA as before.
  + STA never reveals who it really is (at layer 2)
* **Very flexible, easy to add Action frames**
* **Very secure and private**
  + STAs may use “Change” each time which renders any brute force to find IRMK completely moot
  + As STAs associate with a different MAC address and IRM Hash, impossible for a listener to know it is the same STA
* **STAs may always include IRM Check based upon perceived loading of AP/Network**
  + APs can store many IRMKs and use check to down-select.

1. **IRM AND USE CASES**

IRM, IRMA, IRMK and IRM Hash are all described in 21/1585 and 21/1673

Use Cases are provided in 21/0332

Use cases – “user level” view of behaviors and the gap between desired and current behaviors when RCM is used

1. **Pre-association client steering (AP steering, band steering, network steering)**

IRM SATISFIES. Present scheme may rely on the same MAC Address being used such that AP/network knows it is returning. This implies STA has associated before. If STA associated using IRM, the IRMK can be stored. STA using IRM can be identified by the network pre-association. STA can use different IRMAs (and IRM Hash) for each of the multiple APs, but based on sme IRMK.

1. **Post-association access control (Parental controls, etc.) (Out-of-scope)**

IRM SATIFIES. User can choose not to “opt-in” and use “private”, but if using IRM, then network identofes user. Note, the STA associates with a different IRMA every time. Much more secure than using same MAC address each time.

1. **Post-association home automation (including arrival detection (Out-of-scope)**

IRM SATIFIES. User can use IRM, and provide protection against any snooping. Note, the STA associates with a different IRMA every time. Home AP stores the IRMKs for the permitted STAs. Much more secure than using same MAC address each time.

1. **Airport Security Queue (Out-of-scope)**

IRM DOES NOT SATISFY. STA needs to associate to pass over IRMK so no ID in this case as STAs never associate.

1. **Grocery store customer flow analysis (Out-of-scope)**

IRM SATISFIES – Assuming User “Opts-in” to switch on the IRM. The IRMK is then stored for that phone. Note that in this case the AP could store many hundred of IRMKs so the IRMK Check is very useful and the STA should recognize the need to include in IRM elementfor it in this case.

1. **Grocery store frequent shopper notifications (Out-of-scope)**

IRM SATISFIES – Assuming User Opts-in” to switch on the IRM. The IRMK is then stored for that phone. Note that in this case the AP could store many hundred of IRMKs so the IRMK Check is very useful and the STA should recognize the need for it in this case. A higher layer app could easiliy use the IRMK identification to associate the STA to the customer.

1. **Infrastructure (home or enterprise) with different SSIDs per band (not caused by RCM)**

IRM COULD SATISFY – If the AP are in communication with other, they could share the IRMK. Would require the STA to also econize they are same network. If the STA uses same IRMK for both, then problem solved.

1. **Infrastructure (home or enterprise): Probes are randomized, even to/heard by associated AP**

IRM SATISFIES – No reason not to add IRM element to probes. If STA has associated to network, then preassociation IRMK recognized.

1. **Rogue client detection in infrastructure network (Out-of-scope)**

IRM DOES NOT SATISFY, BUT MAY HELP – If same STA uses a different IRMK it is considered a different STA. The rogue would have to associate as “unknown” each time. This may be a clue that the STA needs further investigation.

1. **Rogue APs (Not affected by RCM)**

IRM DOES NOT SATISFY - Not a use case affected by RCM. Rogue APs would only be affected with STAs that have not previously associated to “true” AP. They would not have the IRMK stored. They could respond with “No IRMK found” but this could alert the STA.

1. **Soft AP (No Soft AP in Spec)**

IRM MAY SATISFY – Not sure. IRM could be used as maybe not that many STAs will associate. Not really sure what the “problem” is though.

1. **Onboarding a “known” MAC address (secure environment, or controlled/managed), but does anyone know the address?**

IRM SATISFIES – Use the IRMK to recognize STAs.

1. **Customer Support and Troubleshooting**

IRM SATISFIES – Use the IRMK to recognize STAs.

1. **Residential Wireless Gateway with Hotspot (Out-of-scope)**

IRM SATISFIES – Gateway can use the IRMK to recognize STAs for the home network.

1. **Lawful surveillance (not required to fix)**

IRM DOES NOT SATISFY. In fact, makes Lawful Intercept even harder

1. **Emergency services (pre- or post-association) (not required to fix)**

IRM DOES NOT SATISFY.

1. **Public Wi-Fi hotspot and roaming (AP to AP – is this the same ESS??)**

NOT SURE -

1. **MAC address collisions (WBA)**

IRM SATISFIES – It is the IRMK that matters, so two STAs can use same IRMA but IRM Hash is different and so is the IMK

1. **Accounting and billing issues (WBA)**

IRM SATISFIES –IRMK identifies the STA,

1. **QoS and QoE (WBA)**

IRM SATISFIES –IRMK identifies the STA,

1. **DHCP pool exhaustion (WBA)**

IRM COULD SATISFY – If IRMK was used. Needs higher layer app.

1. **Inconsistent DHCP address assignment (WBA)**

IRM COULD SATISFY – If IRMK was used. Needs higher layer app.

1. **ACLs/firewalls (IP-address based ACL?) (WBA)**

IRM SATISFIES –IRMK identifies the STA,