IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Identifiable Random MAC, IRM  Analysis, Use Cases, Criteria | | | | |
| Date: 2022-01 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Analysis of IRM and Use Cases

Rev 1 – Revised section on analysis against features/attributes/criteria

Summary:

This document provides a complete overview of the IRM scheme and its advantages, together with full analysis of how IRM deals with the TGbh Use Cases. IRM is then examined against each of the criteria in the TGbh Issues Tracking document. Possible spoof attacks are discussed and the effort required to attack the key.

1. - Brief Overview of IRM
2. – Advantages of IRM
3. – IRM and Use Cases
4. - IRM Analysis
5. – Spoof Attacks
   * Non-AP STA Spoof Attack
   * AP Spoof attack
6. – Key Attack

# BRIEF OVERVIEW OF IDENTIFIABLE RANDOM MAC ADDRESS (IRMA)

* STA produces a random 48-bit MAC address from 46 random bits, plus the “01” local admin.
  + Same as any RMA,
  + Termed “**IRMA**”.
  + The STA chooses a new random MAC every association, so the TA, the IRMA, 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.  Therefore, it is impossible for a listening third party to know if this is the same STA as before as it has no resemblance at all to previous associations.
* STA 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” in the IRM Element, 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 is the identity for the STA and is stored by the AP.
  + STA can use different IRMKs for different associations
* 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 same IRM Hash value 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 an IRMK Check field to the IRM element,
  + Allows AP to down-select IRMKs if it has many IRMKs stored.
  + AP can request the IRMK Check to down select IRMKs if not included in IRM Element
  + IRM Check reduces IRMK list by a factor of 256.

# ADVANTAGES OF IRM (over present RCM)

* **A different Random MAC (the IRMA) is used even when returning to same ESS – more privacy!**
  + Even though STA indicates “Known”, 3rd party can not know if same STA as previously (unlike present RCM 11aq scheme “same MAC address for same AP”)
  + MAC address and IRM Hash field values change every time. The last IRMK is remembered at the AP. i.e. IRMK x = STA A
* **An IRM STA can still choose to use “private” random MAC**
  + If no IRM Hash field, then private MAC address in use.
  + Satisfies the “opt-in/opt-out” requirement.
* **STA can change IRMK at any time**
  + Can change IRMK when associated.
  + No way 3rd party can know if IRMK changed. Hence even if brute force used to find IRMK (a huge task), if IRMK changed, impossible to know if same STA reassociates.
    - Huge deterrent to attack
  + AP still knows that it is STA A even though IRMK has changed.
* **AP can restrict its stored list if necessary and request a new IRMK if “No IRMK found”, but IRMK Check means that very large lists can be maintained.**
  + STA can provide old or new IRMK
  + STA could see this as a threat (spoof AP) and react accordingly.
  + However, “IRMK Check” allows AP to keep a large store.
* **IRMK Check allows AP to keep long IRMK lists**.
  + STA could automatically include IRMK Check if it considers AP is a ‘busy AP’, i.e., likely to have many IRMKs.
  + AP can request ‘check’ if it wants to down-select IRMKs (if check not included in IRM element
  + Check provides down selection by a factor of 256
    - E.g. if AP has 1000 stored IRMKs, then list reduced to 4 (only 2 calculations required on average)
  + Check does decrease integrity from 2128 to 2120 – still a huge number requiring huge processing power and time (and still only tells attacker that STA has been there before – which RCM does anyway)
* **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 direct 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 new Action frames if cases arise.**
* **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.
* **Anti-Spoofing ability**
  + STAs can use the IRMK Check as a way to thwart rogue APs. Similarly, APs can use the IRMK Check to verify a STA and prevent a spoof STA.

# 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 also be identified by the network pre-association. STA can use different IRMAs (and IRM Hash) for each of the multiple APs, but based on same 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 identifies user. Note, the STA associates with a different IRMA every time. Much more secure than using same MAC address each time. Third party cannot tell who has joined.

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 could be 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 IRM element.

1. **Grocery store frequent shopper notifications (In scope if opt-in)**

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/account, or simply recognize a ‘frequent shopper’.

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

IRM COULD SATISFY – If the APs are in communication with other, they could share the IRMK. Would require the STA to also recognize they are same network. If the STA uses same IRMK for both, then problem solved. Note that the address IRMA is still different per association.

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 can be recognized.

1. **Unapproved 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 (assuming once detected). This may be a clue that the STA needs further investigation. Rogue would need to have the credentials to join.

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

IRM SATISFIES - Not a use case affected by RCM. Rogue APs would only be affective 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. STA can challenge with the IRMK Check. STA ma=y not be using the same IRMK for everything, so providing a unique IRMK still protect 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 (should not 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 – Probably IRM can be used.

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 IRMK. Of course, two STAs associating with the same MAC Address will cause problems, but that is an RCM problem.

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,

# IRM Analysis against features/attributes/criteria

1. **User Opt-in**

IRM Complies

The IRM element has the “private” indication specifically for opt-in and opt-out. This indicates clearly to the AP that the STA is using an IRMA or a purely random MAC. If User opts-in, then STA indicates “known” or “unknown” and includes the IRM Hash in the IRM element.

1. **Third Party cannot track**

IRM Complies.

Each association, including when returning to a network, uses a different MAC address (IRMA) and different IRM Hash (in the IRM element). A discussion on third party attack is provided below.

1. **No exposure of PII**

IRM Complies.

A STA uses an IRMK as its identifier. The AP can keep a list of IRMKs for particular STAs, e.g., IRMK x = STA A where A is numbered by the AP. The AP then could use upper layer schemes to further identify the STA, if required. A STA can change the IRMK once associated but the AP can still associate that STA with the new IRMK.

1. **Network provides user services – device can return to same ESS**

IRM Complies.

The Network (AP) stores the latest IRMK against pre-associated STAs. The STA also stores the IRMKs it has provided for each network. At the Association Request stage, the AP can start to confirm the IRMK, or it may wait until the STA is associated. The services that the network has cleared for that STA can be provided.

1. **Network can use for troubleshooting**

IRM Complies.

The Stored IRMK is the unique ID for each STA that has associated using an IRMA. The network can identify the same STA even if no PII has been provided.

1. **Network can provide QoS, DHCP, services**

IRM Complies

The Stored IRMK is the unique ID for each STA that has associated using an IRMA. Any services that have been negotiated with that STA can be applied whenever the STA associates.

1. **Pre-association client identification is possible**

IRM Complies

The IRM element may be included in probes and/or association requests. Also the ANQP IRM element is available. As long as the STA has previously associated to the AP and hence an IRMK is stored at the AP, then the STA can be recognized pre-association.

1. **Is “Extensible”**

IRM Complies

The IRM scheme identifies the STA using an IRMK. The AP/network can then use that identification to allow the addition of new capabilities and functionalities.

1. **Processing required on AP one-time/infrequent**

No additional processing is required on a one-time basis.

1. **Processing required on AP each association**

The AP is required to calculate the IRM Hash each time a STA joins with an IRMA, in order to find the associated IRMK. The use of the IRMK Check is designed to reduce the number of calculations by a factor of 256. The IRM Hash calculation is standard as the hash used is the SHA-256/128. The balance is that a third party is required to perform 2119 hash calculations on average to brute force the IRMK, but even then, it is not that useful.

1. **Processing required on non-AP STA one-time/infrequent**

There is no additional processing required by the non-AP STA on a one-time basis.

1. **Processing required on non-AP STA each association**

The non-AP STA is required to perform just one IRM Hash calculation for each association

1. **Set up complexity for AP administrator**

The IRMK effectively replaces the MAC address as the identifier. Hence there is no additional complexity or memory requirement. The AP simply keeps a list of IRMKs associated with STAs. To indicate the support of IRM is trivial.

1. **Set up complexity to configure non-AP STA**

The only new set up task may be the selection of IRMKs and when to change them. This is no more than using random MAC addresses and remembering which networks they apply to. Indicating support for IRM and the associated Action frames is relatively trivial.

1. **Memory Storage requirments on AP**

No more than if storing MAC addresses. Storing IRMKs instead.

1. **Memory Storage requirments on no-AP STA**

No more than if storing random MAC addresses. Storing IRMKs instead.

1. **Third party can determine is non-AP STA is using the solution**

Yes. The STA indicates support for IRM and the IRM element is present.

1. **Solution depends upon encrypted link**

The IRMK is always provided over the encrypted link. Once provided, however, the non-AP STA can be recognized before association and encryption.

1. **How strongly is the ID bound to a user?**

The IRMK identifies the non-AP STA. The IRMK can change however, but the lionk is firm.

1. **Is it important that the AP is trusted?**

The non-AP STA can use different IRMKs for networks (APs) so as to protect against a rogue AP and IRM has much less privacy concerns than using random MAC. In fact, if a spoof AP masquerades as a ‘trusted’ AP, then the non-AP STA can challenge it. Also, as the non-AP STA uses a different MAC address each association the AP cannot tell who it is, as against the RCM case. Separate clauses discussing all spoofing possiblitites and third party attacks and how IRM deals with them, are provided below.

1. **How “real” is the ID, in terms of getting to actual end-user identification versus a throwaway?**

The IRMK is a device identification and does not include any actual end user identification. A STA may change its IRMK at anAP at any time, when associated.

1. **How much can the network can trust the ID, to re-establish context from last time?**

The IRMK provided by the non-AP STA is only when associated. The AP can challenge the IRMK if it is suspicious by asking for IRMK Check. The IRMK only provides an identification of the STA and does not provide any information on the device or user. This is entirely up to the AP and upper layer applications if further information is required. If the network simply needs to know that this is a ‘trusted” STA (i.e., been associated before), the IRMK is sufficient.

1. **How does client know level of trust of network?**

The client, if it associates with “known”, can ‘test’ the AP/network by asking for the IRMK Check. If associating for the first time, i.e., “unknown”, then it is no different from any association using RCM or real MAC come to that, BUT the client can use a different IRMK and does not disclose its identitiy.

1. **Operation with Open of PSK networks?**

Using an IRMA to associate does not disclose who the client is and is more private than using RCM. Also a client may choose to simply use a “private” address. Obviously sending the IRMK for the first time association in an open network means that it could be intercepted but the client can use different IRMKs for each network and the IRMK does not give any information about the user or device. The non-AP STA will be recognized and the network can provide whatever service(s) the user is expecting. The IRMK can also be used for pre-association. The client can protect against a rogue non-AP STA using the IRM Check. A third party listening will not know that the same non-AP STA is re-associating.

1. **Control over lifetime of the identifier? User control and/or network control?**

The client controls the use of its IRMKs. It can change an IRMK for any network, when associated. It may choose to use a time based scheme for when to change the IRMK, there is no restriction.

# Spoof Attacks

## 5.1 Non-AP STA spoof attack

IRM has built-in defensives, if really required, but difficult to see a real threat. IRM provides better protection than RCM.

### 5.1.1. Scenario

Rogue non-AP STA captures the MAC address (IRMA) and IRM element used by the ‘real’ non-AP STA when it associates to an AP. The rogue then uses these to attempt to associate to the AP (presumeably at another time).

Points:

* This is basically no difference to a rogue simply using a copied RCM MAC addess
* The IRMA used by ‘real’ STA does not indicate any information about the user or device (except that it is associating with this AP). Also as the IRMA changes for every association, the rogue cannot know if it the same STA as may have been previously observed.
* The copied IRM element has to be indicating “known” as the rogue does not know the IRMK
* If an open network, then a non-AP STA would know that its IRMK can be copied but the IRMK does not have any information about the device or user. By using a different IRMK than that used for any other network, the non-AP STA can simply make sure it is recognized by the network and not compromise itself.

Difficult to imagine a scenario where the rogue needs to impersonate another STA in an open or ‘weak’ netwrok, BUT

* The rogue must have the Password in order to associate. To assess this attack, it is assumed that the rogue does have access (e.g., displayed password).

### 5.1.2. Effect and IRM counters

Assuming that the rogue can associate, and still wants to impersonate another STA:

* AP can ‘challenge’ the rogue with an IRM Check.
  + - If network is ‘weak’ then AP could do this as a matter of course. (Assuming that it is felt that this is a credible threat)
  + Non-AP STAs do not need to use the same IRMK but can vary them and change them.

If the network is weak, however, then it may be assumed that the IRMK is compromised anyhow, as may be any ID scheme including RCM, i.e., the rogue is listening in to all traffic on the network. However, RCM is using the same MAC Address each time which provides the rogue with a reference, whereas IRM uses different IRMA and rogue cannot be sure who it is.

If the rogue is on the network and monitoring exchanges, then it will recover the ID Query exchange and simply can use this at any time in the future.

The AP network can verify the IRMK and challenge the associating STA. The rogue would have to have stored all previous associations together with all intercepted IRMK exchanges in order to get through the IRMK Check challenge.

### 5.1.3 Conclusion

IRM is better than RCM against a non-AP STA spoof attack. Using IRM it is hard to see a scenario where such an attack is worthwhile. The non-AP STA can still be recognized and not be compromised.

## 5.2 AP spoof attack

IRM makes if difficult/impossible for a rogue AP to recognized the STA unlike RCM which indicates same address for the spoofed AP. IRM has an extra layer of protection not offered by ID Query.

### 5.2.1. Scenario

Rogue AP spoofs an AP that a STA has previously associated with. The rogue AP may want to obtain information on the STA and identify the device or user. Assuming the AP is attractive, the STA may send Association Request with an IRM element. This does not disclose the IRMK.

In order for the STA to associate, the rogue AP would need to have the same security as the AP it is spoofing. In this unlikely event, all bets are off, but if the rogue AP does not have the IRMK listed, then it can ask the STA for a new IRMK giving a reason. The STA may be suspicious and not supply a new IRMK. The IRMK in itself has no information as to the device or user.

A STA pre-associating using an ANQP IRM element, can only be recognized by an AP that has the IRMK stored.

### 5.2.2. Effect and IRM counters

A rogue AP could not identify a STA using IRMA, but if the STA is using RCM, then the MAC address could be recognized. It is assumed that a rogue AP cannot duplicate the same same security, but if it does, then IRM does have one more layer of protection in that the AP must ask for the IRMK and provide a reason. A STA can make a decision as to whether the request is reasonable (e.g., time of last association).

Note that if using ID Query, in this unlikely scenario, the STA will provide the ID.

### 5.1.3 Conclusion

IRM is more secure than RCM and, in the unlikely case that the STA does associate, marginally more secure than ID Query.

# Key Attack

## 6.1 Third Party attack

A third party attempts to determine the IRMK for a STA.

### 6.2. Scenario

A STA that is associating with an AP using an IRMA includes an IRM Hash value in the IRM element where the IRM Hash is calculated using the IRMA and the IRMK (IRM Key) that is stored at the AP. A third party could attempt to determine the IRMK by performing a vaste number of calculations. If the IRMK was found, then the STA may be identified. However, as each STA associates with a new IRMA and IRM Hash, it is not known when the same STA associates again without having to perform the SHA256/128 hash calculations each time.

The IRMK is 128 bits, i.e., 2128 possibilities. If the STA includes the IRM Check, then there are 28 combinations of the 16 bits that satisfy the IRM Check. Hence, although no actual bits of the IRMK are disclosed, the number of IRMK possibilities is effectively 2120, still a huge number.

### 6.3. Effect and IRM counters

Assuming the extremely unlikely event that a third party does determine the IRMK, then it could conceivably try that same IRMK with every STA that associates, with the idea that it would know that it was a STA that associated before. Note, however, the IRMK bears no relationship to the STA device and this is similar to a STA using RCM and associating with the same address.

However, a STA can and should change its IRMK regularly, and this would render any third party IRMK determination completely moot.

### 6.4 Conclusion

Determining the IRMK woud involved tremendous resources with no real reward.

RCM using the same address for the same network is obvious that the same STA is associating, whereas with IRM, the IRMA is different for each association and a third party cannot tell if it is a STA that has previously associated unless it knew the IRMK. As a STA can change the IRMK registered at an AP, then even if a third party decided to find IRMKs rather than mine bitcoins, it is rendered a waste of time if the STA simply changes its IRMK.

Note: 2119 = 6.65 x 1035

1 year = 3.15 x 1019 tera hash