IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Signature-based RCM STA Identification Solution Analyses | | | | |
| Date: 2022-01-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Liuming Lu | OPPO |  |  | luliuming@oppo.com |
| Chaoming Luo | OPPO |  |  |  |
| Lei Huang | OPPO |  |  |  |
| Pei Zhou | OPPO |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission analyzes the signature-based RCM STA identification solution (i.e. signature-based solution) on use cases and features/attributes/criteria.

R0 – Initial discussion document.

R1 –

# Introduction

This document evaluates the signature-based RCM STA identification solution (i.e. signature-based solution), being proposed in TGbh as one candidate solution, per the 11-21/0332r28 (Issues Tracking) document. The solution is described in the 11-21/1083 (Signature-based Method for Identifying STAs with Randomized MAC Addresses) document and 11-21/2039 (Random Index Assisted Scheme) document.

# Solution analysis

## 2.1 Applicability to Use Cases

The following table analyzes the signature-based solution’s applicability to those use cases that are agreed to be in scope, or possibly could be “nice to have” (but not required to be solved), per Issues Tracking document(11-21/0332r28).

**Table 1 – Analysis against Use Cases**

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case # | Use Case Name | Status | Signature-based solution’s applicability to those use cases. |
| 4.1 | Pre-association client steering | “Nice to have” though, if can find sufficient privacy controls (opt-in, etc.) – maybe recommendation? Maybe if a solution to another problem happens to solve this? | Yes, when returning to a network that has previously been visited. |
| 4.2 | Post-association (returning) device identification per network/SSID basis | In scope, (assuming we evaluate criteria): | Yes, STA can be identified by ‘address signature’. |
| 4.3 | Post-association home automation/arrival detection | In scope, (assuming we evaluate criteria): | Yes. Same analysis as for use case 4.2. |
| 4.6 | Grocery store frequent shopper | In scope, (assuming we evaluate criteria): | Yes. Same analysis for use case 4.2, or 4.1. |
| 4.8 | Infrastructure use of probes | Perhaps only recommendations in Spec.  Anything about address in [directed?] probes to other APs in the same ESS when associated? | Yes. Same analysis for use cases 4.1 and 4.2. |
| 4.10 | Approved client in secured environment | Maps partially to post-association use cases, and partially a pre-association issue? | Yes. Same analysis as for use case 4.2. |
| 4.14 | Onboarding a “known” MAC address | Can be solved with 802.1X security, or SAE passwords, or Wi-Fi Easy Connect, or BRSKI (where does the list end – out of band anything?)?.  Might add recommendations to suggest those solutions? | Yes, a “known” MAC address could be identified by ‘address signature’ too. |
| 4.15 | Customer support and troubleshooting | Aspects are within our scope, might be alternative interface(s) to access and/or control the MAC address behavior. | Yes, with user “opt in”. |
| 4.22 | QoS and QoE (WBA) | Can be solved with 802.1X security, or SAE passwords, or Wi-Fi Easy Connect, or BRSKI (where does the list end – out of band anything?)?.  Might add recommendations to suggest those solutions? | Yes, with user “opt in”, assuming the AP QoS/QoE rules is configured using the device identifier. |
| 4.23 | DHCP pool exhaustion | Might add recommendations. | Yes, assuming the device identifier will be used in the DHCP server. |

## 2.2 Applicability to attributes/criteria

The following table analyzes the signature-based solution on the attributes/criteria currently agreed to be useful, per Issues Tracking document(11-21/0332r28).

**Table 2 – Analysis against features/attributes/criteria**

|  |  |  |
| --- | --- | --- |
|  | Attribute/criteria | Signature-based Solution |
| 1 | User opt-in, per network | Yes |
| 2 | Third-party (attackers/parties not intended to have the identification) can’t track – device can use a different address when returning/over time | Yes, ‘address signature’ changes when device use a different MAC address. |
| 3 | No exposure of PII that had been hidden by RCM? | Yes. |
| 4 | Network can provide user services (automation, access control, etc.) – device can return to same ESS | Yes. If STA has associated before, the STA’s certificate has been stored. When STA returns with a different RMA, it can be identified by the AP. |
| 5 | Network can use for troubleshooting | Yes. |
| 6 | Network can provide QoS, DHCP, services | QoS, yes.  DHCP, yes if the device identifier is used in the DHCP server. |
| 7 | Pre-association client identification is possible (nice-to-have??) | Yes, with ‘address signature’ in the authentication frame of PASN (Preassociation security negotiation). |
| 8 | Is it “Extensible”? (Nice-to-have?) | Maybe. |
| 9 | Processing required on AP one-time/infrequent | AP receives and caches the STA’s certificate at the ‘first’ association.  If ‘Random index assignment’ method is also used, AP allocates and sends random indexes to the STA. |
| 10 | Processing required on AP each association | Verifies (by using hash and ECC functions) the ‘address signature’ using each certificate in the cache list.  If ‘Random index assignment’ method is also used, a simple look up is needed and reduces the number of certificate trials. |
| 11 | Processing required on non-AP STA one-time/infrequent | STA sends its certificate at the ‘first’ association. |
| 12 | Processing required on non-AP STA each association | Generates (by using hash and ECC functions) the ‘address signature’.  If ‘Random index assignment’ method is also used, a random index is selected and added to the authentication frame. |
| 13 | Setup complexity for AP administrator | Only turn on/off the RCM with signature. |
| 14 | Setup complexity to configure non-AP STA | Only turn on/off the RCM with signature. |
| 15 | Memory/storage requirements on AP (consider large # of clients) | Storage of certificate of each STA, only for associated clients.  Each certificate may be around 400+ octets. |
| 16 | Memory/storage requirements on non-AP STA | Storage of STA’s certificate, |
| 17 | Third-party can determine if non-AP STA is using the solution? | Yes. The STA indicates that ‘address signature’ field is present in frames. |
| 18 | Solution depends on an encrypted link? (Nice to have if ‘no’?) | No. The STA’s certificate is transmitted in Authentication frame, and the Authentication frame is not encrypted. |
| 19 | How strongly is the ID bound to a user, and giving the user access/capabilities/etc.? | Depends. This solution does not provide the exact format or value of the identifier for a STA. STA or user could choose anything unique as the identifier along with its certificate. |
| 20 | Is it important/critical that the AP is trusted? | Yes. A rogue AP that pretends as a trusted AP could obtain STA’s certificate. Therefore, it is critical that the AP is trusted. |
| 21 | How “real” is the ID, in terms of getting to actual end-user identification versus a throwaway? | Depends. This solution does not provide the exact format or value of the identifier for a STA. STA or user could choose anything as the identifier along with its certificate. |
| 22 | How much the network can trust the ID, to re-establish context from last time? (Spoofing protection) Level of trust of the ID should match the trust of the data exchange with this network. | Highly trustable. The STA’s certificate cannot be forged by a third-party and is very secure. The ‘address signature’ can only be generated by the STA’s private key, and will not be forged by a third-party. |
| 23 | How does client know level of trust of the network (trust of AP/infrastructure/back-end entities)? | The STA does not know the level of trust of the network. |
| 24 | Consider operation of the solution on networks that are “Open”, or PSK and could be exposed. (Note that protection of (post-association/SA) identifier is no higher than protection of the data exchange. Not a new problem caused by RCM.) | In this signature-based solution, the STA’s certificate is transmitted in Authentication frame. The network that are “open”, or PSK does not add additional risk for this solution. |
| 25 | Control over lifetime of the identifier? User control and/or network control? | The STA’s certificate has a relatively long lifetime, which is controlled by the certification authority.  STA or user could change its identifier while keeping its certificate unchange. |
| 26 | Consider whether solution offers identifier per device, user or group. | per STA. |
| 27 | Network being spoofed can gain access to client identifier? | If a spoof AP pretends as a trusted AP, the network can obtain the STA’s certificate, so it can recognize STA through STA’s certificate. |

**References:**

[1] 11-21-0332r28, Issues Tracking

[2] 11-21-1083r0, A Signature-based Method for Identifying STAs with Randomized MAC Addresses

[3] 11-21/2039r0 Random Index Assisted Scheme for Reducing RCM STA Identification Complexity

[4] IEEE P802.11az™/D4.0 August, 2021