Ongoing developments in IEEE 802.11 WLAN standardisation

A study group on randomized and changing MAC addresses

Amelia Andersdotter (Chair, RCM TIG, IEEE 802.11)[1]

HotPETS, Stockholm, July 2019

[1] amelia.andersdotter@dataskydd.net

Disclaimer

All views presented here are the views of the presenter, and should not be misconstrued as public statements by the IEEE, IEEE-SA or IEEE 802.11 or any other group participating in discussions under the auspices of any of these organsations.

Privacy work in IEEE 802.11

Privacy features have recently gained traction in IEEE 802.11, the leading global standards body for wireless local area networks (WLAN).

Examples include work on Recommendations for Privacy Considerations (P802E) in IEEE 802.1 and the recently adopted Pre-Association Services amendment .11aq (available for purchase since July 2018).

This presentation highlights some ongoing work.

Privacy Recommendations P802E

(Very) roughly inspired by IETF RFC6973.

Work in progress since 2014.

Drafts sadly not public.

Intended to support (eventually) privacy and security work
through-out the standards development process.

Privacy Recommendations P802E

(Very) roughly inspired by IETF RFC6973.

Work in progress since 2014.

Drafts sadly not public.

Intended to support (eventually) privacy and security work
through-out the standards development process.

Privacy Recommendations P802E

(Very) roughly inspired by IETF RFC6973.

Work in progress since 2014.

Drafts sadly not public.

Intended to support (eventually) privacy and security work through-out the standards development process.

Privacy Recommendations P802E

(Very) roughly inspired by IETF RFC6973.

Work in progress since 2014.

Drafts sadly not public.

Intended to support (eventually) privacy and security work
through-out the standards development process.

More information

https://1.ieee802.org/security/802e/

Older documents: https://mentor.ieee.org/privecsg/documents

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- ☑ Reseed the OFDM scrambler when MAC address changes

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- ☑ Reseed the OFDM scrambler when MAC address changes
- ☑ Choose random MAC address to associate to an AP and retain that MAC address during the connection to the ESS

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Pre-Association Services amendment .11aq Privacy Enhancements

- ☑ Randomize MAC address pre-association
- ☑ Not probe for specific SSIDs
- ☑ Reset the sequence number counter used to identify MSDUs and MMPDUs when the MAC address changes
- ☑ Reseed the OFDM scrambler when MAC address changes
- ☑ Choose random MAC address to associate to an AP and retain that MAC address during the connection to the ESS
- ☑ Set MAC address to a previously used (random) MAC address when attempting to use some state on the AP bound to the previous MAC address

Deeper overview:

https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx

Challenges during and after adoption of .11aq

1) Work is based on results from research community from 2013 and onwards...

2) Privacy enhancements created a lot of controversy.

3) It interferes with use-cases of important users of .11 standards.

4) RCM TIG is a topic interest group - a discussion forum - to hash out possible future work for IEEE 802.11 to

   ❋ Define and address these use-cases
   ❋ Discuss lingering .11aq controversies(???)
   ❋ Request future/more privacy work(???)

   It remains to be seen (in second half of 2019)...

❀ Standards are not mandatory. They are voluntary.

❀ Developing standards takes time, money and commitment.

❀ The standards are written by those who show up but...

❀ ...their impact is determined by whether they are implemented.

Get more information:

https://mentor.ieee.org/802.11/documents?is_dcn=DCN%2C%20Title%2C%

20Author%20or%20Affiliation&is_group=0rcm

QUESTIONS?