IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of a Few Comments |
| Date: 2022-07-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolution to a few easily resolved (in the eye of the author) comments.

**CID 21**

Comment:

What is the meaning of "foil traffic analysis" in the context of the sentence?

Proposed Change:

None

Discussion:

Searching for the term “traffic analysis” using a popular search engine received: “Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication, it can be performed even when the messages are encrypted. In general, the greater the number of messages observed, more information be inferred.”

Which is about right. The addition of padding to the identifier, prior to encrypting, and the recommendation in Z.4 to use a pad length that differs from the pad the last time the identifier was encrypted, will ensure that intercepted and examined messages will not be able to be combined to deduce information that might be deduced if a constant length was always used for opaque identifiers.

Proposed Resolution:

Reject. The use of this term in Z.2 is consistent with its use in other sections as well as the common definition of the term. No proposed change was suggested and none is needed.

**CID 22**

Comment:

"The overhead added to each frame by the scheme is 16 octets of AES-SIV tag plus length of tweak plus one octet of padding indication plus padding. For an 8 octet tweak that would be 25 octets."

The overhead octets are not clear. According to text, it should be (for 8 octet tweak):

 16 (Tag) + 8 (tweak) + 1 (padding indication) + K (padding)

Does blob (ID) have a fixed value or variable value? It would be better to indicate the exact overhead so the vendors would take overhead into consideration when implementing.

Proposed Change:

None

Discussion:

The scheme described in annex Z does not assume any identifier size, whether fixed or variable. The size of the identifier would not be considered overhead of a privacy-protecting scheme since that identifier is the thing being protected and the overhead is that which must be added in order to protect the thing.

So annex Z does already describe the exact overhead to the fullest extent possible—again, padding is variable and the length of the tweak will be fixed for a particular instantiation of the scheme. The overhead is the AES-SIV tag (which will always be 16) + the length of the tweak + 1 length in indicate the pad length + the length of the pad. If your tweak is 8 octets then it’s 25 + the length of the pad. What could be more clear?

Proposed Resolution:

Reject. The exact overhead is described as closely as possible. It cannot be more clear.

**CID 23**

Comment:

"There is a single symmetric secret, k, shared by all APs in an ESS."

Should we consider how to derive this key?

Should we consider how to share this key with all APs in an ESS?

Should we consider updating the key with all APs in an ESS?

Proposed Change:

None

Discussion:

Short answer: no, no, and no. ☺

Longer answer: *how* is irrelevant and this annex in informative so normative statements would probably not be appropriate; we do not discuss these sorts of things in 802.11 (e.g. see FT and how the PMK hierarchy gets shared among APs in the ESS) since they are out of scope and 11f never really did take off; updating is similarly out of scope.

Proposed Resolution:

Reject. Specification of how this key is managed is unnecessary and out-of-scope.

**CID 34**

Comment:

At the end of this sentence it would make sense to have a reference to Annex Z.

Proposed Change:

Add "(see Annex Z)" before the full stop at the end of the sentence.

Discussion:

Yes, it does make sense to do this.

Proposed Resolution:

Accept.

**CID 54**

Comment:

"Without modification" is unnecessary; if it is modified then it is not the identifier. The identifier is the value.

Proposed Change:

Delete "without modification".

Discussion:

Yes, it is unnecessary. Just removing it makes the rest of the sentence somewhat clunky though.

Proposed Resolution:

Revised. *Instruct the editor to modify section 12.2.11 as indicated:*

For other cases, the non-AP STA sends the identifier, if it has one and opts-in to using it, during the initial 4-way handshake in the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4. The non-AP STA shall send the most recently received value from an AP in the ESS.

**References:**