IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of Padding CIDs |
| Date: 2024-06-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This document proposes resolution to two CIDs on the nature of padding being used in the Annex.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3137 | RISON, Mark | 51.57 | AF.2 | "The maximum amount of padding is determined by the size of identifier being padded and the value of n, and is equal to 237 minus the sum of the length of the identifier and n. " -- it is not clear where 237 comes from.  Also, units are missing but assuming 237 is in octets then there seems to be a dimension error since n is in bits, although it is only defined later on in the subannex | Change to "Any amount of padding can be added, as long as the resulting opaque identifier can fit in the Device ID element (in the Device ID field thereof)." | Revised: Changes to the Device ID definition have not been reflected in the annex. The value is 231, not 237. 253 is largest body of an element but device ID eats up 5 more of those leaving 248 for a maximum device ID. Minus 1 for the pad length and 16 for SIV’s tag and it’s 231. Incorporate changes in <this document>. |
| 3183 | RISON, Mark | 51.51 | AF.2 | It is not clear whether the amount of padding is itself required to be random | Clarify | Revised: Add “The amount of padding to add varies and its variability determines the resistance to traffic analysis that this scheme provides.” per <this document>. |
|  |  |  |  |  |  |  |

*Instruct the editor to modify AF.2 as indicated:*

**AF.2 Generation of opaque device identifiers**

There is a single symmetric secret, k, shared by all APs in an ESS. The length of k is 256 bits if AES-SIV-256 is used or 512 bits if AES-SIV-512 is used. In either case, the procedure is to prepend the identifier with a single octet indicating the number of random octets of padding that follow. The amount of random padding to add varies and its variability determines the resistance to traffic analysis that this scheme provides. For example, if there are 4 octets of padding added to mitigate traffic analysis, the identifier, id, might be padded as:

 padded-id = 0x04 0xc8 0x34 0x9a 0x70 <id>

If there is no padding, a single zero octet is prepended to the identifier.

The padded identifier is prepended with a variable length input comprised of random octets called a tweak. The length of the tweak in bits, n, determines the baseline security of the scheme such that the probability of a duplicate identifier being generated, assuming a worst case of no padding, would be 1/2(n/2).

The maximum amount of padding is determined by the size of the identifier being padded and the size of the tweak in octets and is equal to 231 minus the sum of the lengths of the identifier and the tweak (231 is 248, the largest Device ID possible, minus 1 for the pad length, and minus 16 for the encryption overhead).

For example, an 8 octet tweak would provide collision resistance of at least 1/232 (in addition to that provided by the padding) and the tweaked-padded-id would be constructed as (assuming the values of the tweak are generated according to Annex J.5):

 tweaked-padded-id = 0x7e 0x17 0x54 0x82 0xf1 0xd0 0xaa 0x52 0x04 0xc8 0x34 0x9a 0x70 <id>

The tweaked-padded-id is then passed to AES-SIV in deterministic mode as plaintext using k as a key to

produce the opaque device identifier.

**References:**