IEEE P802.11
Wireless LANs

Abstract

This document proposes resolution to the ongoing discussion on the nature of padding being used in the Annex. And resolves CIDs 4008 and 4009.

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

Abstract

This document proposes resolution to the ongoing discussion on the nature of padding being used in the Annex.

*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-id 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). Padding of the tweaked identifier increases the security of the scheme.

The overhead of the scheme is 17 octets—1 for the pad indicator and 16 for the SIV tag—plus padding and plus the size of the tweak. Device identifiers that are greater than 233 octets cannot be opacified using this scheme.

Note: 233 is the maximum size of a device ID with no padding and no tweak minus the overhead. The resulting opaque identifier needs to fit in a Device ID KDE.

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:**