IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of a Few Annex AD CIDs | | | | |
| Date: 2023-09-05 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Proposed resolution of CIDs 76, 130, 261, and 262

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 76 | Technical | 0 | AD.1 | 40 | 29 | The introduction to this annex could more clearly describe what is being generated, i.e., relate it more closely to the procedure by using the same terms. | Change the firs sentence to read "This annex provides an example for generating an identifier for the Device ID field of the Device ID element (see 9.4.2.307a) as used in the procedure defined in 12.2.11.1 (Device ID indication). |
| 130 | Technical | 0 | AD.2 | 41 | 1 | "tweak" is not a defined term in 802.11; although it is used elsewhere, in the context of encryption and key derivations. | Change "tweak" to "ciphertext" |
| 261 | Technical | 0 | AD.2 | 41 | 1 | "variable-length tweak" consisting of what? | Change to "variable-length tweak comprised of random-valued octets". |
| 262 | Technical | 0 | AD.2 | 41 | 6 | Undefined reference | Change "Appendix J.5" to "Annex J.5." |

***Discussion***

CID 76: This is a much better introduction. Accept.

CID 130: The tweak is not ciphertext. It becomes part of the ciphertext but it is a random, probabilistic input to AES-SIV. Since AES-SIV is operating in deterministic mode, encryption of the same plaintext with the same key would produce the same output. For long-term identities that would enable tracking. So the tweak adds a security parameter to the process—longer tweak, less probability of repeating. An intro/definition of the tweak is added. To further enhance security it is proposed to make the pad be random as well. Revised, see 11-23/1500r0.

CID 261: Good comment. Wordsmithing to make it harmoniously work with the resolution to CID 130. Revised, see 11-23/1500r0.

CID 262: Yes, that’s true. Accept.

***Instruct the editor to make the following changes to Annex AD:***

**AD.1 General**

This annex provides an example for generating an identifier for the Device ID field of the Device ID element (see 9.4.2.307a) as used in the procedure defined in 12.2.11.1 (Device ID indication). The requirements for using those procedures are that the identifier precludes tracking by third parties. In addition to satisfying those requirements, this scheme also provides for countermeasures to deal with traffic analysis, precludes cutting-and-pasting of identities into conversations, prevents the same identifier from being used on distinct ESSs, and has an acceptable security level based on the birthday paradox. It uses symmetric cryptography for speed and DoS resistance. It imposes minimal overhead on each frame and imposes minimal state retention requirements on an ESS (a single secret), and a binding of each unwrapped identity assigned to a STA and the current opaque device identifier provided to it.

Opaque identifiers are generated and processed by APs. To a non-AP STA they are indistinguishable from a random string and have no significance.

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

The identifier generation scheme takes a unique identifier as input and uses AES-SIV in deterministic mode to wrap the identifier to produce output.

There is a single symmetric secret, k, shared by all APs in an ESS. The length of k is either 256 bits or 512 bits depending on whether AES-SIV-256 or AES-SIV-512 is used. In either case, the procedure is to prepend the identifier with a single octet indicating the number of randomoctets of padding that follow. For example, if there are 4 octets of padding added to mitigate traffic analysis, the identifier, id, would be padded as:

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

If there is no padding, a single octet of the value zero 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, *n* in bits, 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). For example, an 8 octet tweak would provide collision resistance of at least 1/232 (in addition to that provided by the padding) and would be constructed as (assuming the values of the tweak are generated according to AnnexJ.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. The authenticating tag produced by AES-SIV is embedded in the output ciphertext and becomes part of the opaque device identifier.

**AD.3 Processing of opaque device identifiers**

All APs in an ESS use the same tweak length for all opaque device identifiers which are generated and parsed.

APs that receive opaque device identifiers using the procedures described in 12.2.11 (Changing MAC Address), pass the opaque device identifier to AES-SIV with key k. If AES-SIV returns FAIL, the protocol using the opaque device identifier fails. If AES-SIV returns a plaintext, the (known-length) tweak is removed and the next octet, the pad length, is inspected to determine how many additional octets are removed to recover the original identifier, id. This identifier is checked to ensure that the non-AP STA’s identity uses the current opaque identity that was received. If so, the unwrapped identity is passed up to the protocol using the scheme with an indication of success.

**References:**