IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Annex Text for Opaque Device ID | | | | |
| Date: 2022-03-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes an Informative Annex to describe a scheme to generate opaque device identifiers for use with the Network Generated Device ID proposal of 11bh.

*Instruct the editor to obtain an Annex section header, replace <ANA> with it, replace TBD with the section designation describing the network generated device id, and incorporate the following into the TGbh draft:*

**<ANA> Example opaque device identifier scheme**

(informative)

**<ANA>.1 General**

This annex describes an example opaque identifier scheme to be supplied for use with the Privacy Protection procedures in clause TBD. The requirements for using those procedures are that the identifier preclude 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.

**<ANA>.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 zero octets of padding that follow. For example, if there are 4 octets of padding added to foil traffic analysis, the identifier, *id*, would be padded as:

*padded-id = 0x04 0x00 0x00 0x00 0x00 <id>*

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

The padded identifier is the prepended with a variable-length tweak. The length of the tweak, *n* in bits, determines the 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 and would be constructed as (assuming the values of the tweak are generated according to Appendix J.5):

*tweaked-padded-id = 0x7e 0x17 0x54 0x82 0xf1 0xd0 0xaa 0x52 0x04 0x00 0x00 0x00 0x00 <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.

**<ANA>.3 Processing of opaque device identifiers**

APs that receive opaque device identifiers using the procedures described in section TBD, 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 (static-lengthed) tweak is removed and the next octet 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.

**<ANA>.4 Using opaque device identifiers**

An AP that receives an opaque device identifier will extract the original identity and generate a new opaque device identifier for the STA. It is recommended that a new opaque identifier is generated with a pad length that differs from the pad length of the previously wrapped identifier.

The AP associates the new opaque identifier with the non-AP STA’s identity.

**<ANA>.4 Security of scheme**

The security guarantees of AES-SIV mean that it is computationally infeasible for an adversary to generate a valid opaque device identifier that could be processed by an AP and it is computationally infeasible for an adversary to decrypt a valid opaque device identifier.

Assuming the combination of tweak and pad are never repeated for a given id, the probability of a given identity producing an opaque device identity that has been used already is at least 1/2(n/2) where *n* is the number of bits of tweak. This probability can be lessened further by using different amounts of padding each time an identity is wrapped.

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.

**References:**

11-22-0154-00-00bh-opaque-device-id

11-22-0187-02-00bh-network-generated-device-id