IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of some security comments |
| Date: 2019-03-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE` | 3333 Scott boulevardSanta Clara, CaliforniaUnited States of America | +1 888 555 1212 |  |
|  |  |  |  |  |

Abstract

This submission proposes resolution to a few security comments.

**CID 2142: PMKID field**

“There are 9 references to ‘PMKID field’. Not sure what this is, as I can only find a ‘PMKID list’ or ‘PMKID count’. At these 9 locations could someone sort out what is being refered to? I supsect it is the PMKID list field.” with a proposed change of “At 9 locations replace ‘PMKID field’ with ‘PMKID list field’”.

Discussion: Yes, it is the PMKID list field except that it’s List and capitalization is really really critical.

Proposed resolution: Revised, “At 9 locations replace ‘PMKID field’ with ‘PMKID List field’”.

**CID 2363: FD RSN subfield**

“There are some references to an "FD RSN subfield" but no such subfield exists” with a proposed change of “Change ‘FD RSN subfield’ to ‘FD RSN Information subfield’ in 11.46.2.1, 11.46.2.2 and 12.12.2.2.”

Discussion: Yes, it is the FD RSN Information subfield.

Proposed resolution: Accept.

**CID 2531: Finite field element field**

“’Finite field element’ is confusing because it looks like it's referring to an 802.11 element” with a proposed change of “Change ‘Finite field element (FFE) field’ to ‘FFE field’ throughout.”

Discussion: The confusion exists because the clarifying word “field” was removed in the comment. When one refers to the blob of bits as defined it is the “finite field element field” which does not sound like an 802.11 element. A “finite field element” is a cryptographic term of the art, it refers to an element in a finite field. This finite field element is contained in a different thing that is also called a field. It is unfortunate that this word is overloaded but using an ackronym is not clarifying. The description of the “finite field element field” describes what it is.

Proposed resolution: Reject.

**CID 2689: PMKID privacy considerations**

“In PMKSA caching, STA sends one or more PMKIDs in the clear in (Re)Assoc Request frame (or Auth frame in FILS case). In cases where PMK lifetime and caching period are long, the same PMKID might be sent each time a STA connects to the same AP/network, and this could be used by bad actors to track a user's location with privacy implications.” with a proposed changed of “Provide means by which, e.g. during each auth/assoc procedure, the AP can securely provision STA with a randomly-generated pseudonym for the PMKID which the STA uses on the next auth/assoc with that AP.”

Discussion: The STA is required to associate with the MAC address it used when the PMKSA to which the PMKID refers was established. Making a pseudonymous PMKID would be somewhat pointless when the MAC address can be used by bad actors to track a user’s location.

Proposed resolution: Reject.

**CID 2221: who has a MAC address?**

“Authenticators and Supplicants don't have a MAC address, the STA does.” with a proposed change of “Change the definition of authenticator address to ‘... of the IEEE 802.1X Authenticator's STA’

Change the definition of supplicant address (P168.20) to ‘... of the IEEE 802.1X Supplicant's STA’”.

Discussion: this sounds like the result of a long discussion in ARC which need not be repeated here.

Proposed resolution: Accept.

**CID 2551: Quadruplicated text**

“’To prevent key reinstallation attacks, a non-AP STA in which dot11WNMSleepModeActivated is

true shall maintain a copy of the most recent GTK and most recent IGTK ‘ -- should not quadruplicate this statement, even less so with variant wordings. We did not duplicate the statement for the original KRACK fix” with a proposed change of “In 11.2.3.16.1, 12.7.7.4, 12.12.2.1, 13.5.1 delete the para starting (#1321) and replace it with ‘NOTE---See 6.3.19 regarding prevention of key reinstallation attacks.’”

Discussion: KRACK was the result of people not reading the standard fully and implementing a component protocol or API by just reading the subclause that described the component protocol or API. It is not reasonable to assume future implementers will do anything different.

Replacing this normative text with an informative note that directs the reader to another part of the standard does not seem right, it’s almost asking for the problem to arise again. Also, section 6.3.19 says nothing about “prevention of key reinstallation attacks” so adding an informative note to point people to non-existent text seems like a really bad idea.

Finally, there does not seem to be a problem with being explicit and repetitive like this. In fact, it is kind of emphatic. So the combination of no existing problem and a problem created by accepting the proposed change means reject.

Proposed resolution: Reject.

**References:**