IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of Some More Security Comments | | | | |
| Date: 2014-01-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA 94089 | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission proposes resolution to CIDs 2240, 2330, 2331, 2491, 2577, 2962, 3000, 3262

***Instruct the editor to modify section 4.5.4.2 as indicated:***

**4.5.4.2 Authentication**

SAE authentication, FILS authentication, and Open System 802.11 authentication are used by non-DMG STAs in an RSN for an infrastructure BSS.

***Instruct the editor to modify section 8.4.2.189 as indicated:***

**8.4.2.189 Fragment element**

Each information element is limited to a maximum of 255 octets since their length field is a single octet (Figure 8-104). If data to be represented in an IE is too large and the generic advertisement service (GAS) is not used, it is necessary to fragment the data (see section 9.33 and 9.34).. The format of the Fragment IE is indicated in Figure 8-183du (Fragment IE).

***Instruct the editor to delete sections 8.4.2.189.1 and 8.4.2.189.2, including Table 8-183ak***

***Instruct the editor to change the headings of sections 9.5 and 9.6 as indicated:***

**9.5 Frame Fragmentation**

**9.6 Frame Defragmentation**

***Instruct the editor to insert new sections 9.33 and 9.34***

**9.33 Element Fragmentation**

The general format of elements limits the size of each element to 255 octets. Data that is too large for a single element may be fragmented into a series of elements consisting of the original element into which the data would not fit, immediately followed by a number of Fragment elements.

The data to be fragmented is divided into M + N chunks, where

• M is the result of the integer division of the length of the data by 255

• N is equal to 1 if the length of the data modulo 255 is greater than 0, and equal to 0 otherwise

The original element into which the data would not fit is filled with the first chunk of data and is termed the leading element. The length of the leading element shall be 255. This element is immediately followed by M-1 Fragment elements, each containing the next chunk of data and with a length of 255. If N = 1 these elements are immediately followed by the last chunk of data in a Fragment element which has a length equal to the length of the data modulo 255.

A Fragment element shall only follow another element whose length is 255. A Fragment element shall not be fragmented.

**9.34 Element Reassembly**

Elements which have had their information fields fragmented are those that are followed by one or more Fragment elements. To reconstruct the original data the chunk of data from the leading element is concatenated, in order, with the chunks of data from the series of Fragment elements that follow it. The reassembly procedure finishes when any element other than a Fragment element is encountered or the end of the MMPDU is reached.

***Insruct the editor to modify section 11.5.1.3.2 as indicated:***

**11.5.1.3.2 Security association in an ESS**

* In the case of FILS authentication, the STA repeats the same actions as for initial contact and authentication. Note that a STA can take advantage of the fact that it can initiate FILS authentication to multiple APs while maintaining a single association with and finishing t FILS authentication with, one AP.

***Instruct the editor to modify section 11.11.2.1 as indicated:***

**11.11.2.1 Discovery with FILS authenticaiton**

A STA that discovers a FILS-capable AP that advertises a public key (see section 8.4.2.183) that the STA trusts, or has an ability to gain trust through validation of an X.509v3 certificate, may begin the FILS Authentication protocol to the AP and perform mutual authentication using trusted public keys.

***Instruct the editor to modify section 11.11.2.2.2. as indicated:***

**11.11.2.2.2 Key establishment with FILS public key authentication**

First, the public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5. Then the public key, as a group element, shall be verified in a group-specific fashion according to section 5.6.2.3 of SP 800-56a.

**References:**