IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment Resolutions: CID 4088 | | | | |
| Date: 2014-03-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr., San Diego, CA 92121 | +1 858 651 6645 | gcherian@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This submission proposes resolution to CID 4088

|  |  |  |  |
| --- | --- | --- | --- |
| 4088 | what is the probability of collision using CRC-32() truncated to 2 octets? What happens if there's a collision? | use a real hash function with a reasonably low probability of collision or explain what happens when a collision occurs. | The probability of collision only depends on the number of octets used. The distribution CRCs generated from different strings is sufficiently random (see last page of document) |
|  |  |  |  |

* FILS Aauthentication and higher layer setup capability indications [CID 2869]

In Beacon and Probe Response and FD frames, a FILS iIndication element is included by an AP with dot11FILSActivated value of true. FILS iIndication element indicates properties of the FILS authentication protocol used and also indicates if concurrent IP address assignment is performed by the AP. The IP address type is also indicated. [CID 4787]

When FILS shared key authentication[13/1354r2] is used, an AP can indicate up to 7 domains[CID 2380] that the AP is connected to using the hashed domain name field of the Domain Information field of the FILS Indication element. The domain name is set to the domain[CID 2380] as defined in IETF RFC 6696. For each of the indicated domain names, the FILS element carries a 2 octet hash of the network domain name and the IP address type of the corresponding domain. The hash of the domain name ([CID 2726]RFC 1035 “c” compliant) is computed as follows:

H = L(CRC-32(ToLowerCase(D)),0,16) [CID 2092 (ed note, this is exactly as presented in the resolution but is it right?)]

where:

H is the Hashed Domain Name,

L is defined in 11.6.1,

CRC-32 is defined in 8.2.4.5,8.2.4.7 (Frame Body field), [CID 4086]

ToLowerCase is the function that converts upper case characters to lower case

D for AP is either:

* NAI Realm as defined in NAI Realm field of NAI Realm Data field format in NAI Realm ANQP-element format (8.4.4.10) Or
* Home network realm as defined in [3GPP TS 23.003] for WLAN as included in advertised in 3GPP Cellular Network ANQP Element.

D for non-AP STA: NAI Realm used in the EAP-Response/Identity of the initial full EAP authentication

For each domain, the type of IP address available is also indicated in  8.4.2.181 (FILS IP Address Assignment element). [CID 3047]

* Authentication discovery of a FILS capable AP[CID 2974]

An AP indicates that it is capable of performing FILS Aauthentication by including FILS Indication element in[CID 2490] Beacon or Probe rResponse frames. FILS-capable Beacons or Probe rResponses framesshall contain an RSN element advertising the FILS Aauthentication AKM. [CID 2972][CID 4726, 4727]

When shared key authentication[13/1354r2] is used, AP may advertise up to seven realms using a 2-octet hashed domain name of the domain information of FILS Indication element in Beacon, Probe Response and FILS Discovery frames. If the STA discovers a FILS-capable AP that advertised a hashed domain name that matches the hashed value of the realm of the third party authentication server with which the STA shares a valid rRK as defined in IETF RFC 6696, the STA may begin the FILS authentication protocol with the AP. The domain name hashing is specified in 10.44.4 (FILS Aauthentication and higher layer setup capability indications). [13/1312r4, CID 3127][CID 2973]

A STA that discovers a FILS-capable AP that advertises a public key (see 8.4.2.177 (FILS Public Key element)) that the STA trusts, or has an ability to gain trust through validation of an X.509v3 certificate, may begin the FILS Aauthentication protocol to the AP and perform mutual authentication using trusted public keys.[14/003r3]

….

* Key establishment with FILS shared key authentication [13/1354r2]

…

Step 1: STA requirements:[13/1510r2]

If the STA chooses to initiate FILS shared key authentication, the STA first chooses a random 16 octet nonce. It then determines whether to attempt PMKSA caching. If so, it generates a list of one or more PMKSA identifiers, otherwise it[14/052r2] constructs an EAP-Initiate/Re-auth packet as specified in IETF RFC6696, with the following additional clarification: [13/1354r2]

* Regarding EAP-RP Flags
* The B flag shall be set to 0, indicating that this is not an EAP-RP bootstrap message. [CID 2102]
* The L flag shall be set to 1, indicating that the TTP with whom the STA shares the rPK is to provide the lifetimes of rPK and rMSK in the EAP-Finish/Re-auth Packet. [13/1354r2]
* The Cryptosuite field shall not be set to 1. [CID 2101]

If PFS is desired, the STA selects a finite cyclic group from the dot11RSNAConfigDLGGroupTable, generates an ephemeral secret private key, and performs the group's scalar-op (see 11.3.4.1 (General)) with its random ephemeral private key and the generator from the selected finite cyclic group to compute an ephemeral public key.

The STA then constructs an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2] and the Authentication transaction sequence number set to one (1). The [13/1514r1]random nonce shall be encoded in the FILS nonce field (see 8.4.1.57 (FILS Nonce field)), and the FILS authentication type shall be set to indicate the specific type of FILS authentication.If PMKSA caching is being attempted, the PMKID list shall be constructed out of the list of PMKSA identifiers that are shared with the target AP, otherwise, the EAP-Initiate/Re-auth packet shall be copied into the FILS [CID 2873] wrapped data field (see 8.4.2.184 (FILS Wrapped Data element)). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)) and the ephemeral public key shall be encoded in the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion). [14/0052r2

The STA shall transmit the Authentication frame to the AP.

Step 1: AP requirements [13/1510r2]

Upon reception of the Authentication frame, the AP shall do the following: [13/1510r2]

If Authentication frame includes a Finite Cyclic Group field, then the AP shall first determine whether the indicated finite cyclic group in the received FILS authentication frame is supported. If not, it shall respond with an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2] and the Status set to 77 (Authentication is rejected because the offered finite cyclic group is not supported) and shall terminate the exchange. If the group is supported or if PFS is not being used in this exchange, the AP shall check whether PMKSA caching is being attempted by the presence of the PMKID list element. If so, the AP checks whether any PMKSA identifier offered in the PMKID list matches an identifier for a cached PMKSA. If not, the AP shall respond with an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Status set to 53 (invalid PMKID) and shall terminate the exchange. If PMKSA caching is not being attempted, the AP shall [14/052r2]extract the EAP-Initiate/Re-auth data from the FILS [CID 2873] wrapped data field (see 8.4.2.184 (FILS Wrapped Data element)) and shall forward it to the Authentication Server. When applicable, the AP communicates with the Authentication Server using the same protocols [CID 2715]it uses when authenticating with EAP. Suitable protocols include, but are not limited to, remote authentication dial-in user service RADIUS (as specified in IETF RFC 2863-2000) and Diameter (as specified in IETF RFC 6942-2013).[13/1510r2][CID 2729]

If PFS is being used, the AP shall also generate an ephemeral private key and perform the group's scalar-op (see 11.3.4.1 (General)) to produce its own ephemeral public key. The AP may delay the generation of its ephemeral public/private key pair until after receiving a response from the Authentication Server, if applicable[14/052r2].

Authentication Server procedure:[13/1510r2]

When PMKSA caching is not being used, the Authentication Server processes the EAP-Initiate/Re-auth packet as specified in RFC6696 and returns an EAP-Finish/Re-auth packet to the AP. In the case of successful authentication by the Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet.

Step 2: AP requirements[13/1510r2]

If the AP is not connected to, or does not recognize the Authentication server identified by the STA using the realm in the keyName-NAI field of the EAP-Initiate/Re-auth message, then the AP shall send Authentication frame with Status set to <ANA+1>, “Authentication rejected due to Unknown Authentication Server” to the non-AP STA.

If the Authentication Server responds with a failure indication, then the AP shall produce an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2] and the Status set to 15 (Authentication rejected because of challenge failure). If the Authentication Server responds with a success indication (including the associated EAP-RP rMSK), then the AP shall generate its own nonce and construct an Authentication frame for the STA. This frame shall contain the FILS wrapped data which encapsulates EAP-Finish/Re-auth packet received from the Authentication Server. In addition, if PFS is used, the Element field of the Authentication frame sent by the AP contains the AP's ephemeral public key. In this frame, the AP shall set the Authentication sequence number to (2).[13/1510r2]

[14/052r2] [14/0341r5]If PFS is being used for the exchange, then the AP shall perform the group's scalar-op (see 11.3.4.1 (General)) with the STA's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss.

Upon transmission of the FILS Aauthentication response, the AP shall perform key derivation per 11.11.2.3 (Key derivation with FILS authentication).

Step 2: STA requirements[13/1510r2]

The STA processes the received Authentication frame as follows.[13/1510r2]

* If the received Authentication frame does not include the Authentication algorithm number equal to "Fast Initial Link Setup authentication"<ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2], or if the Status is set to <ANA+1>, “Authentication rejected due to Unknown Authentication Server”, if PMKSA caching was attempted and the received Authentication frame does not include a PMKID list, or if PMKSA caching was not attempted and [14/052r2]the received Authentication frame does not include an EAP-Finish/Re-auth packet, then the STA shall abandon the FILS authentication
* If the received Authentication frame includes the Status equal to 15 (Authentication rejected because of challenge failure)or 53 (invalid PMKID), then the STA shall abandon the FILS authentication
* The STA ensures that the AP transmitted PFS parameters consistent with the desire of the STA (indicated by whether or not the STA transmitted an ephemeral public key).
* If the STA transmitted an ephemeral public key, and the received Authentication frame does not include a well-encoded ephemeral public key, then the STA shall abandon the FILS authentication.
* If the STA did not transmit an ephemeral public key desired PFS, and the received Authentication frame includes an ephemeral public key, then the STA shall abandon the FILS authentication.
* If applicable, the STA processes the EAP-Finish/Re-auth packet as per RFC6696 -
* If the 'R' flag = 0, indicating success, then the STA shall generate rMSK.
* If the 'R' flag = 1, indicating failure, then the STA shall abandon the FILS authentication.
* If PFS is being used for the exchange, then the STA shall perform the group's scalar-op (see 11.3.4.1) with the AP's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss.
* The STA shall perform key derivation per 11.11.2.3 (Key derivation with FILS authentication) and key confirmation per 11.11.2.4 (Key confirmation with FILS authentication) [CID3085].

If the STA doesn't successfully receive Authentication response within the time of dot11AuthenticationResponseTimeOut, [CID2874,2979] then the STA should perform retransmission procedure as defined in IETF RFC 6696. If the retransmission procedure fails, then the STA shall abandon the FILS authentication and should perform full EAP authentication via IEEE 802.1X authentication. [CID 2980]

Step 3 [13/1510r2]

This step is part of Key confirmation. At this step, the STA generates the Association Request frame to the AP as specified in 11.11.2.4 (Key confirmation with FILS authentication). The STA may also include FILS HLP Container element or FILS IP Address Assignment element to request IP address. [13/1510r2] [14/0423r0][CID 4821]

Step 4 [13/1510r2]

This step is part of Key confirmation. At this step, the AP generates the Association Response frame to the STA as specified in 11.11.2.4 (Key confirmation with FILS authentication). The AP may also include FILS HLP Container element or FILS IP Address Assignment element to assign the IP address for the STA. [13/1510r2] [14/0423r0][CID 4821] [13/1510r2][14/052r2]

***Insert new row (prior to last row) in Table 8-42 as follows:***

|  |  |  |
| --- | --- | --- |
| * Status codes | | |
| Status | Name | Meaning |
| <ANA> |  | Authentication rejected due to FILS authentication failure. |
| <ANA+1> |  | Authentication rejected due to Unknown Authentication Server. |