IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Fixing Some SAE Issues | | | | |
| Date: 2019-05-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott Boulevard  Santa Clara, California,  United States of America |  |  |
|  |  |  |  |  |

Abstract

Release of the “Dragonblood” paper caused the SAE text in 802.11 to be read very carefully. That resulted in identification of some errors that need correcting.

Comment: the text on generating a quadradic residue and a quadratic non-residue is backwards.

Discussion: yes it is!

***Instruct the editor to modify section 12.4.4.2.2 as indicated:***

**12.4.4.2.2 Generation of the password element with ECC groups**

This technique involves creation of a quadratic residue, qr , and quadratic non-residue, qnr , prior to beginning of the hunting-and-pecking loop. These values can be chosen at random by checking their legendre symbol:

do {

qr = random() mod p

} while ( LGR(qr | p ) is not equal to 1)

do {

qnr = random() mod p

} while ( LGR(qnr | p ) is not equal to -1)

Comment: According to section 12.4.5.2 the scalar will always be greater than 1 but when it is processed the verification check is whether it’s greater than 0. Both RFC 5931 (EAP-pwd) and RFC 7664 (Dragonfly key exchange) verify the scalar as being greater than 1. What is it? > 0 or > 1?

Discussion: It should be > 1. Since a properly formed scalar cannot be the value 1 (per 12.4.5.2) fix the verification text.

***Instruct editor to modify section 12.4.5.4 as indicated:***

**12.4.5.4 Processing of a peer’s SAE Commit message**

If the scalar value is greater than 1 and less than the order, r, of the negotiated group, scalar validation

succeeds; otherwise, it fails.

**References:**