|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Resolution for Some Security CIDs | | | | |
| Date: 2014-07-17 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON | +1 (415) 690-7363  +1 (647) 867-5658  Skype: rstruik | [rstruik.ext@gmail.com](mailto:rstruik.ext@gmail.com) |

Abstract

This document discusses some security-related LB#201 comments related to D2.0 of the TGai specification.

**Summary sheet: Suggested resolution of a selection of comments from 14/565r14:**

|  |  |  |
| --- | --- | --- |
| **CID#** | **Resolution** | **Brief rationale** |
| 5025 | Accept | Revise wording of AEAD algorithm reference in key confirmation text |
| 5029 | Revised | Provide more details on certificate processing during key confirmation |

**DETAILS: Suggested resolution of a selection of comments from 14/565r14:**

**CID #5025:** (Rene Struik) 11.11.2.4.1, p. 112, l. 40:

(TR) Clause 11.11.2.4.1, p. 112, l. 40: Replace "AEAD encryption operation" by "AEAD algorithm" (after all, the ciphertext also provides for authentication assurances). Suggested remedy: see comment.

Suggested resolution: Revised.

Note: This is labeled as Revised, rather than Accept, since the comment applies to the corresponding paragraph of 11.11.2.4.2 as well.

***Change Clause 11.11.2.4.1 as follows:***

The plaintext passed to the AEAD encryption algorithm is the data that would follow the FILS session element

in an unencrypted frame. If the AEAD cipher requires a unique counter, the current value of the AEAD

counter from the PTKSA shall be passed to the AEAD encryption algorithm. The ciphertext output by the

AEAD ~~encryption operation~~ algorithm becomes the data that follows the FILS session element in the encrypted and

authenticated 802.11 Association Request frame. The resulting Association Request frame shall be transmitted

to the AP.

***Change Clause 11.11.2.4.2 as follows:***

The plaintext passed to the AEAD encryption algorithm is the data that would follow the FILS session element

in an unencrypted frame. If the AEAD cipher requires a unique counter, the current value of the AEAD

counter from the PTKSA shall passed to the AEAD encryption algorithm. The ciphertext output by the

AEAD ~~encryption operation~~ algorithm becomes the data that follows the FILS session element in the encrypted and

authenticated Association Response frame. The resulting Association Response frame shall be transmitted to

the STA.

**CID #5029:** (Rene Struik) 11.11.2.4.1, p. 112, l. 64:

(TR) Clause 11.11.2.4.1, p. 112, l. 64: The behavior in case verification of the certified public key, including policy checks, fails is not described. Suggested remedy: Specify certificate verification details.

Suggested resolution: Revised.

Note: This comment applies to the corresponding paragraph of Clause 11.11.2.4.2 as well.

Discussion: The current draft only talks about verifying the signature, but not about this in sufficient detail. It should specify that verification includes   
a) checking the signature applied by the communicating party in the key confirmation message (e.g., simple ECDSA signature verification).  
b) checking the entire certificate chain, so as to check validity of all certs, both cryptographically (e.g., check ECDSA signature for each one) and from a policy perspective.  
This should also specify that processing fails if any of these checks are not successful.

***Change Clause 11.11.2.4.1 as follows:***

For FILS public key authentication~~, the AP uses the STA's (certified) public key from the FILS Public Key~~

~~element to verify that the contents of the Key-Auth field of the Key Confirmation element consist of a hash~~

~~of a concatentation of the STA's public Diffie-Hellman value, the AP's public Diffie-Hellman value, the~~

~~STA's nonce, the AP's nonce, the STA's MAC address, and the AP's BSSID, in that order, using the negotiated~~

~~hash function. The specific technique for verification depends on the crypto-system used by the public~~

~~key.~~ , the AP uses the STA's (certified) public key from the FILS Public Key

element to verify that the signature contained in the Key-Auth field corresponds to the purported signature by the STA over the concatenation of the following:

* the STA's public Diffie-Hellman value gSTA,
* the AP's public Diffie-Hellman value gAP,
* the STA's nonce NSTA, the AP's nonce NAP,
* the STA's MAC address STA-MAC, and
* the AP's BSSID AP-BSSID

in that order, according to the signature scheme used. Furthermore, the AP checks all certificates in the certificate chain, both cryptographically and from a security policy perspective, according to the procedures for checking certificates and certificate chains in RFC 5280. If any of these verifications fail~~s~~, authentication shall be deemed a failure.

***Change Clause 11.11.2.4.2 as follows:***

For FILS public key authentication, ~~the STA uses the AP's (certified) public key from the FILS Public Key~~

~~element to verify that the contents of the Key-Auth field of the Key Confirmation element consists of a hash~~

~~of a concatentation of the AP's Diffie-Hellman value, the STA's Diffie-Hellman value, the AP's nonce, the~~

~~STA's nonce, the AP's BSSID, and the STA's MAC address, in that order, using the negotiated hash function.~~

~~The specific technique for verification depends on the crypto-system used by the public key.~~ the STA uses the AP's (certified) public key from the FILS Public Key element to verify that the signature contained in the Key-Auth field corresponds to the purported signature by the AP over the concatenation of the following:

* AP's public Diffie-Hellman value gAP,
* the STA's public Diffie-Hellman value gSTA,
* the AP's nonce NAP,
* the STA's nonce NSTA,
* the AP's BSSID AP-BSSID, and
* the STA's MAC address STA-MAC

in that order, according to the signature scheme used. Furthermore, the AP checks all certificates in the certificate chain, both cryptographically and from a security policy perspective, according to the procedures for checking certificates and certificate chains in RFC 5280. If any of these verifications fail~~s~~, authentication shall be deemed a failure.