MACsec Ascon Cipher optimization

Reducing the number of permutations for Integrity Only and Integrity and Confidentiality.[1]

Mick Seaman
mickseaman@gmail.com

[1] Please note: Some suggestions in this note are definitely tentative, aimed at getting the discussion going. Do not assume this is implementation ready.

Introduction

P802.1AEef/D1.0 'Integrity Only' and 'Integrity with Confidentiality' both include 4 SecTAG octets in associated data, *A*, for Ascon-AEAD128[1]:

- Sub-optimal, with more permutation rounds than necessary [2]
  - A first Ascon 16 octet block of DA+SA+SecTAG looks neat, but …
  - 12 round, p[12], initialization, 8 round, p[8], for *A* and *P* (plain text) 16 octet Ascon data blocks, and p[12] finalization.
  - Last data blocks of *A* **and** *P* padded to 16 octets before permutation
  - If already a 16-octet multiple an extra padding block and p[8] added
- Proposal to move 2 SecTAG octets to IV, or alternatively to omit 2 octets from initial block.
  - This presentation advocates the latter.

[1] As specified in NIST SP 800-232

[2] As pointed out by Alexander Zeh in private correspondence and ballot comment on P802.1AEef/D1.0 with accompanying tutorial information in https://www.ieee802.org/1/files/public/docs2026/ef-zeh-mendel-ascon-partitioning-0526.pdf.

Reducing '*A*'

P802.1AEdf/D1.0 Reducing 'Integrity + Confidentiality's 16 octets of associated data by one or more octets avoids a padding block and p[8].

- Could move SecTAG TCI and SL (2 octets) to *N* (128 bit AEAD-128 nonce), but makes initialization TCI/SL dependent, impacts opportunity to initialize before frame receipt.
- Pre-initialization, spreading work over time, particularly under continuous heavy load is practical if only change in *N* is the MACsec XPN (Extended Packet Number).[1,2] Can reduce peak processing requirement and reception delay.
- The MACsec EtherType in each frame's SecTAG is checked independent of cryptography (to recognize the MACsec protection), so can be easily omitted from A.
- Omitting EtherType also helps interesting case for 'Integrity Only'.

[1] While the MACsec TCI includes information on the Integrity and Confidentiality applied to each protected frame, that is to facilitate network management (without access to data keys) and is not changed by MKA for the duration of an SC (Secure Channel) and certainly not while a given SAK (data key) is being used.

[2] SL dependency would be particularly annoying for sensors and the like protecting small amounts of frame data.

Permutation count

Count of the number of Ascon permutations for P802.1AEef/D1.0 and D1.1 (Editor's draft[1] showing omission of MACsec EtherType from *A*). Unprotected frame sizes include MAC DA, SA, and user data.[2]

Octets[a]	1.0 I-only	1.1 I-only	1.0 I+C[c]	1.1 I+C[d]
13-27	40 (A<=31)	40 (A<=31)	40 (P<= 15)	32 (P<= 15)
28-29	48 (A<=47)	40 (A<=31)	48 (P<= 31)	40 (P<= 31)
30-43	48 (A<=47)	48 (A<=47)	48 (P<= 31)	40 (P<= 31)
44-45	56 (A<= 63)	48 (A<=47)	56 (P<= 47)	48 (P<= 47)
46-59	56 (A<= 63)	48 (A<= 63)	56 (P<= 47)	48 (P<= 47)
60-61	64 (A<= 79)	56 (A<= 63)	64 (P<= 63)	56 (P<= 63)
62-75	64 (A<= 79)	64 (A<= 79)	64 (P<= 63)	56 (P<= 63)

[1] Available at https://www.ieee802.org/1/files/private/ef-drafts/d1/802-1AEef-d1-1.pdf

[2] User data includes user's initial EtherType or other protocol identifier, but excludes any subsequent Ethernet MAC padding—so a min sized unprotected Ethernet frame is 60 octets in the above list.

[a] p[12] initialization and p[12] finalization throughout. [c] A = 16 octets p[8]+p[8]. [d] A = 14 octets p[8].

gg