MAC Data Security

Mick Seaman

mickseaman@gmail.com

MAC Data Security

MACsec (as standardized)

- SecTAG fields and use (review/recap)
- Usable over arbitrary virtual LAN support

MAC Data Security[1]

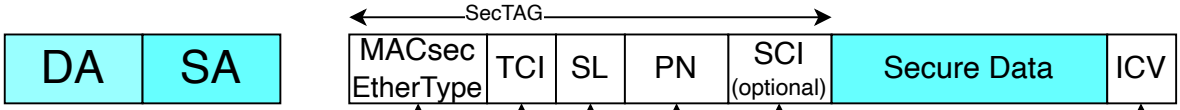
- Usable over arbitrary transport
- Uses existing SecTAG fields

[1] Not attached to this name, but it should clearly distinguish this work from arbitrary application of AEAD (Authenticated Encryption with Associated Data) to network protocols which is out of 802.1 scope.

MACsec (recap)

Data can be added before the MAC Destination Address (or indeed any where in the frame) , by the MAC or other transport carrying the protected frame between 'SecY's (MAC Security Entities) as long it is removed prior to validation.

DA & SA can affect forwarding of both this and subsequent frames, so are integrity protected as are other fields shown cryptographically or by explicit check). CipherSuite determines detail.



Protocol identification, could have been any value unique in the context of the recipient.

(9.5) E(ncrypted), C(hanged) for analysis w/o data key access. E=1 & C=0 can carry MKA (e.g. 11.8).

'Short length'. Supports bridging e2e to wireless MACs, constrained device support. Two possibly spare bits.

32 bit Packet Number, cryptographic nonce (part). XPN extension roll-over, MKA recovery of upper bits if sync lost (> 2 secs disconnect).

Cryptographic Integrity Check Vector (Tag). 16 octets (preferred).

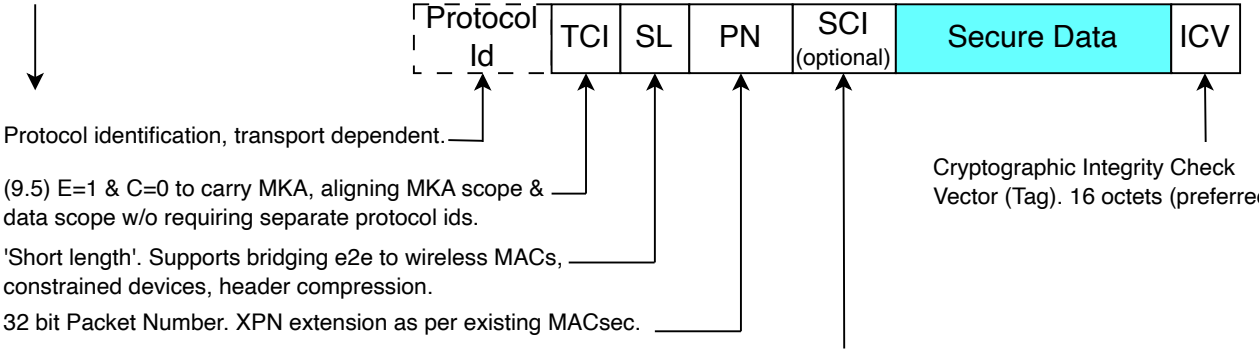
Secure Channel Identifier, cryptographic nonce (part). Unique (MKA verifies) for each transmitter using given SAK (data key). System ID (usually MAC address, but can be other/randomly gen.) + 'Port ID' for multiple SCs from single device (separate physical or virtual network attachments) for p2mp (e.g. 11.8), hot standby (verified operation before switchover), active load splitting (e.g. using link aggregation), or FRER (Frame Replication and Elimination for Reliability 802.1CB).

Data Integrity, optional Data Confidentiality. Data Origin Authenticity from data key possession resulting from authentication/authorization. Cryptographic coverage/operation determined by CipherSuite (selected by Key Server using MKA), not by data frame fields.

MAC Data Security (proposed)

Provides MACsec-like security for current deployments that are not LAN or virtual LAN-based (original MAC DA & SA not carried by transport). SecTAG unchanged except for MACsec EtherType. **Defined by new CipherSuites.**

Fields prior to TCI are determined by the transport protocol, can be modified/added/removed by transport, and are not cryptographically protected. Data origin authenticity from data key possession (distributed by MKA, tied to prior mutual authentication.



Secure Channel Identifier, as per existing MACsec. Can use MAC Address, random generation, or transport derived fields. Only strict requirement is uniqueness amongst users of a given data key. Distinct values for different physical or virtual ports, which will be different for different transport paths, supporting network admin. Inclusion optional, but recommended for p2p. Strongly recommended for p2mp and mp2mp, though TCI SC bit could indicate transport specific generation. As for MACsec multiple SCs from single device support hot standby, active load splitting, FRER.

Data Integrity, optional Data Confidentiality. Data Origin Authenticity from data key possession resulting from authentication/authorization (not by frame fields).

Summary

Existing SecTAG fields applicable to transport scenarios which do not carry/depend on participant's MAC Addresses.

- Create additional Cipher Suites to support this.
- MKA already advertizes participants' Cipher Suite capabilities, and supports Key Server selection.
- Trivial if any MKA parameter addition for SCI variants.
- Transport field addition before or after MDsec is not externally visible behavior (not conformance issue), skipping or adding can be keyed by SCI internally.
- Transport specific selection of protocol id.
- Separate standard (not confusing/altering existing MACsec) but cross-reference .1AE for existing concepts.