MAC Privacy protection

P802.1AEdk amendment to IEEE 802.1AE MAC Security.

Mick Seaman, Chair 802.1 Security Task Group
mickseaman@gmail.com

Overview for 802 Technical Plenary, January 2022.

P802.1AEdk currently in Task Group ballot.

MAC Privacy protection—goal

Reduce correlation of user data frame:

- MAC addresses
- Sizes
- Transmission

with

- individuals
- network applications
- network application details
- levels of application activity.

Following up on exposures described in IEEE Std 802E—Recommended Practice for Privacy Considerations for IEEE 802 Technologies.

MAC Privacy protection—background

Privacy/confidentiality sensitive users

Highly motivated adversaries with considerable resources

MACsec integrity + confidentiality + non-standard extensions

‘Hop-by-hop’ protection

Transmission generally (not exclusively) over fixed links (fiber or service provider) with same guaranteed b/w availability

No need to obscure confidentiality + privacy protection use

Desire for standard, readily available, solution

Leverage existing MACsec

Coexist, so far as practicable, with TSN

Privacy protection protocol

Interface stack ‘shim’ over MACsec (under Link Aggregation)

- Encapsulates user data frames (DA & SA of peer shims)
- Can be separate privacy protection device, but best as MACsec collocation
- Can pad, aggregate, and fragment user data frames before MACsec transmit
- Can use separate MACsec Secure Channels supporting preemption if rqd.

Reception

- Conformant receiver can recover all validly encoded user data frames
- Encoding restrictions on fragment size, in order reception, for feasibility

Transmission

- Range of transmission strategies possible, no need to negotiate with receiver
- Support of two for conformance:
  - — Privacy Frame: Address encapsulation plus optional pad to boundary.
  - — Privacy Channel: Regular transmission of fixed sized, aggregating PDUs

  Selection of either (or None) by user data frame priority.

  Privacy Channel tx interval shaped to allow interfering higher priority tx