MAC Privacy Protection Overview

P802.1AEdk amendment to IEEE 802.1AE MAC Security.
Currently in Working Group Ballot

Editor Don Fedyk dfedyk@labn.net
Chair 802.1 Security TG and Editor Mick Seaman mickseaman@gmail.com
MAC Privacy Goals

With standard Encryption:
   Packet sizes, Frequency and addressing still allows observers to correlate activity and events

Goals: Reduce the correlation of user data frames based on:
• User MAC addresses
• Frame/packet Sizes
• Transmission timing 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 for sensitive users
  • Facing Highly motivated adversaries with considerable resources

• Today:
  • MACsec integrity + confidentiality + non-standard extensions
  • ‘Hop-by-hop’ protection

• MAC Privacy:
  • 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 a standard, readily available, solution
  • Leverage existing MACsec and PAE
  • 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 required.
- Extensible Encoding of MAC Privacy Components

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

Figure 20-2—PrY architecture
Privacy Frame Example

Privacy Frames hide original Frame Headers while adding a little delay (Similar to Existing MACsec)
Privacy Channels Examples

Channel Privacy Hides the complete outward appearance at the cost of some added delay.
Encoding Details

Figure 19-5—MPPDU component encoding

Figure 19-6—Frame Fragment

IEEE 802.1 MAC Privacy Protection