Encrypted Data Stream Formats

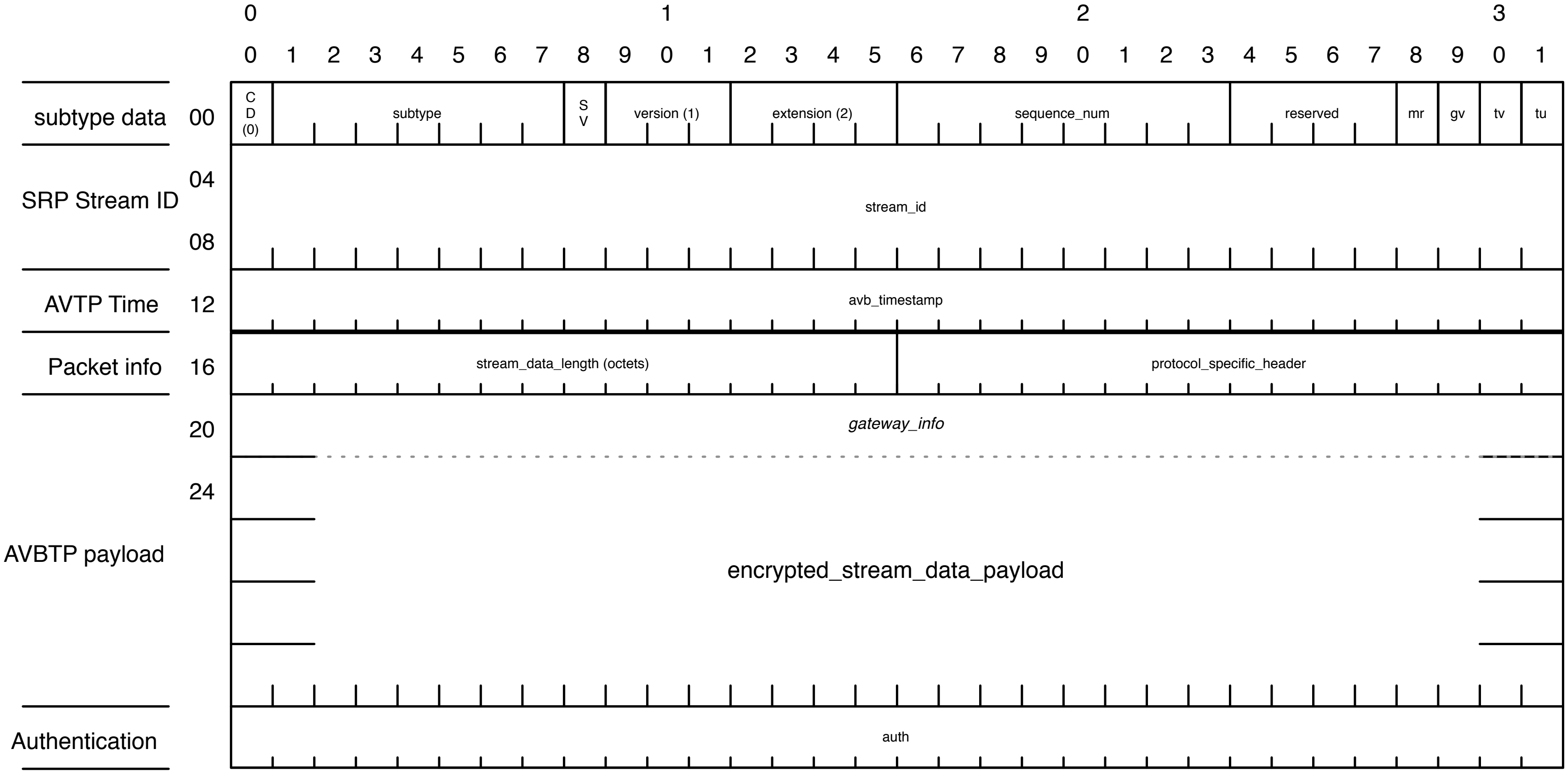
Chris Pane - IEEE 1722A Technical Working Group
May 29, 2013

Justification & Goals of Proposed Format

- Currently proposed encryption solution encrypts entire packet.
    - Great for command traffic (i.e. IEEE 1722.1).
    - Not ideal for data streams.
        - Adds a minimum of 12 extra bytes per packet which reduces maximum number of streams on network by 10-20 percent (AM824, 48K, single channel streams).
        - The proposed encryption method, Elliptic Curve Cryptography (ECC) is not well suited to higher rate traffic (data).
            - Too computationally complex – In many cases, CPU's would require additional hardware acceleration.

- Proposed solution Goals
    - All specified 1722A Formats could be made to leverage the proposed encryption scheme.
    - Protect the data payload while sacrificing minimal stream capacity (adding only 4 bytes).
    - Reduce computational burden on talker/listeners

Proposed PDU Format



0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

subtype data 00: C D (0) | subtype | S V | version (1) | extension (2) | sequence_num | reserved | mr | gv | tv | tu

SRP Stream ID 04 08: stream_id

AVTP Time 12: avb_timestamp

Packet info 16: stream_data_length (octets) | protocol_specific_header

20: *gateway_info*

AVBTP payload 24: encrypted_stream_data_payload

Authentication: auth

Proposed PDU Changes to Support Stream Data Encryption

- Based on AVTP common stream data AVTPDU header format (version 0) and 1722A proposed Version 1 extension.

  - Move mr,gv,tv bits moved to make room for extension field (proposed extension=2)

  - Move gateway_info field into the encrypted payload to secure against leaking possible private data, which if leaked could resulted in Man in the Middle (MIM) attacks.

  - Payload is encrypted with AES-GCM (NIST 800-38D) using the timestamp and the stream ID (XOR'd) as the Initialization Vector (IV).

  - Add auth field to hold the resulting authentication tag (T). This field will be the last 4 bytes of the packet, following the encrypted_stream_data_payload. The Additional Authentication Data (AAD) also referred to as A in GCM equation is composed of the concatenation of the subtype data, Destination Address (DA), Source Address (SA), protocol_specific_header