Pathway Secure Streaming ACN

Scope

An extension to E1.31 to allow authenticated transmission of E1.31 traffic.

Overview

The proliferation of networking equipment in entertainment venues has increased the likelihood of unauthorized access to an entertainment network. This may be caused by a connection, intended or accidental, to the Internet. It may also be caused by a security breach of a wireless network required for use of a console remote focus application.

The addition of a cryptographic hash message digest to each E1.31 packet allows the integrity of a transmitted packet to be verified. With the transmitter and receiver sharing a secret password unauthorized transmitters can be detected and ignored by receivers.

For authenticated traffic three objectives must be met :

1. Sender Authenticity – The identity of the sender must be provable.
2. Data Integrity - It must be possible to detect packets that have been modified during transport.
3. Prevention of replay attacks. It must be possible to detect and reject resent packets that have been previously captured from the network.

To accomplish the first two requirements a message digest is appended to the packet using a cryptographic hash algorithm along with a secret password. A receiver with knowledge of this password can repeat the hashing process and compare the result with the received message digest.

This document does not specify how a password is loaded into each device; Implementers should take appropriate precautions (eg. encryption) if this secret is transported across a network. The third objective is achieved by adding a transmitter sequence to each packet. Note that this sequence is per transmitter (as identified by the CID in the Root Layer) and is not required to be synchronized between sources.

Summary of Changes From ANSI E1.31

Root Layer Protocol on UDP (EPI 17)

The size of post-amble field shall be set to 28 bytes

The Vector field shall be set to 0x50430001. This is a Manufacturer (Pathway Connectivity) specified protocol.

Post Amble field contents shall be :

Field Size (bytes)	**Field Name**
4	Key Fingerprint
1	Sequence Type
7	Sequence
16	Message Digest

Key Fingerprint : Hash of the shared secret
Sequence Type : The Sequence Type used by the transmitter for this universe
Sequence : A seven byte sequence value
Message Digest : The message digest calculated from UDP payload byte 0 thru to the end of Sequence inclusive.

Key Fingerprint

The secret password has a length of 32 bytes. If shorter than 32 bytes pad with null. The resulting 32 byte key is then hashed using the un-keyed blake2s hash function set to generate a 4 byte hash output. This key fingerprint is used by the receiver to select the correct password to use when validating the received packet.

Sequence

The purpose of the sequence is to prevent replay attacks. Transmitters shall select one of the following sequence types and set the sequence type and value accordingly. Receivers shall validate the received sequence as specified below.

Time Based Sequence Type

A sender that wishes to use time as the basis for sequencing packets shall set the Sequence Type field to 0. The sequence field shall be set to the current time in milliseconds elapsed since January 1, 1970, 00:00.0 UTC. Implementers of transmitters are advised to consider how they will prevent this sequence from going “backward” as this may cause receivers to reject their packets.

The receiver shall verify that the received sequence is greater than the previously received sequence from this sender (CID) before accepting the packet. If a receiver has a source of time further checking of a valid “window” may be added but is beyond the scope of this document.

Volatile SequenceType

A sender that wishes to use a simple incrementing sequence shall set the Sequence Type field to 1 and initialize the sequence field to 1 before beginning transmission of a stream. For each successive packet the sender shall increment the sequence field.

The receiver shall track the previous valid sequence from each sender (CID) and compare the received sequence value. The receiver shall verify that the received sequence is greater than the previously received sequence from this sender before accepting the packet. Upon stream termination or timeout according to the requirements of E1.31 the receiver shall initialize its previous valid sequence for this type of sender to 0.

If a sender using this sequence type is rebooted there may be a delay before the receiving devices reset their sequence and begin accepting packets again.

Non-Volatile Sequence Type

A sender that wishes to use a non-volatile sequence type shall set Sequence Type field to 2. Senders using a non volatile sequence type must guarantee that they will not send a lower value than they have sent before. This may be accomplished using a boot count value that is maintained by the device that is shifted into the upper range of this sequence field. The exact mechanism used by the sender to create the non-volatile sequence is beyond the scope of this document.

The receiver shall track the previous valid sequence from each sender (CID) and compare the received sequence value. The receiver shall verify that the received sequence is greater than the previously received sequence from this sender before accepting the packet. Receivers may, but are not required to, store the previously received sequence value for this sender in non-volatile memory. This would allow the receiver to detect a replay attack even though the receiver has been rebooted.

Message Digest

The message digest is calculated using the Blake2s cryptographic hashing algorithm as specified in RFC7693. The Blake2s algorithm was chosen for its speed and simplicity. The secret password has a length of 32 bytes. If shorter than 32 bytes pad with null. The resulting key is provided to the hashing function as the key. The entire UDP payload preceding the Message digest is hashed to a 16 byte message digest using the keyed blake2s hash function