Telecommunication Standardization Sector
Original: English
(TSS)

AVC - 826 Intel-2

Experts Group for Video Coding and Systems in ATM and Other Network Environments

October 24-27, 1995

STUDY GROUP 15
CONTRIBUTION

Source: Jim Toga, Intel Corporation
email: jim_toga@ccm.jf.intel.com
voice: +1 (503) 264-8816
fax: +1 (503) 264-3485

Title: Comments for H.323 Encryption

Date: October 9, 1995

Section 9.2.1 (last paragraph)

Problem/Motivation

The current proposal for media encryption is to encrypt all of the 'multiplexed' streams together, this is dubious due to the following reasons. H.323 is not required to have a single, multiplexed media stream; in many implementations H.323 might have separate physical and logical streams. There may be many reasons to encrypt one media stream and not others within the same conference. This is greatly facilitated by the separate streams.

In H.233 media channel encryption is based upon type and not logical channel number. This will be problematic in a multicast environment in which one or more of a media 'family types' is encrypted, but not all of them. One solution is to specify the media sub-channel in a finer grained manner; i.e. use logical channel numbers as opposed to the broader 'media type' classification.

Solution

H.323 currently specifies that the media identifier (from H.233) uses binary value of 0 [00000000] to represent the encrypted, fully multiplexed signal. Due to the fact that multiplexing may not occur at a physical or logical level in the H.323 world, a new media identifier needs to be defined. The 8th bit (MSB) is currently defined as reserved and unused (being initialized to 0). I propose that this bit be set to one (1) to indicate that the media identifier is now represented in terms of a logical channel number. This does not preclude the use of H.233 bits that define individual media types (audio/video) to specify all logical channels that carry that media type.

If the 8th bit is set in the **media identifier** this indicates the following encoding. The normal tuple of 3 bytes containing **media identifier**, **algorithm identifier**, and **parameter identifier** (each with one byte respectively) will be replaced by a tuple of 5 bytes containing **media identifier, algorithm identifier, parameter identifier**, and a 16 bit value, **channel identifier**.

An alternative is to enhance the command set of H.233 with a analogous command identifier to **Algorithm capabilities (P8)**, this could be coded as **(P10)** and would look the same as specified above (within the context of P8). This might protect parsers that incorrectly parse the unused 8th bit.

Section 9.2.2

The second paragraph is not needed.

Section 9.2.4

The second paragraph will not map to the H.323 context. In order to synchronize a new IV with the media stream the synchronization mechanism will rely on RTP packet sequence numbers. Un-ordered delivery necessitates relying in a packet tagging mechanism to order the IV packet with any subsequent encrypted media packets. This implies having the H.233 implementation extract this information from the RTP header in order to provide the encryption synchronization.

Section 9.2.5

Due to the fact that the encryption synchronization will not be centered around a stream but a packet, it is not clear that this section is necessary. The **encryptionIVrequest** should be allowed at anytime as long as the syncronization steps are used as outlined in **9.2.4** above.