draft-noisternig-ipdvb-ulesec-01

A lightweight security extension for the ULE protocol

Michael Noisternig (University of Salzburg)
Bernhard Collini-Nocker (University of Salzburg)

presented by Gorry Fairhurst at IETF72

Overview

- defines extension header format
  - low bandwidth overhead (6 bytes required)
  - ready for unidirectional & multicast (K bit)
- suggests default security algorithms
  - to foster interoperability
  - low-cost implementation (only AES-128 encryption)
  - addresses issues from requirements draft:
    - data confidentiality, identity protection (passive attacks)
    - data integrity, [source] auth., [replay prot.] (active attacks)
- specifies SA/SP processing
  - simple to implement
  - ready for 1-n/m-n communication (group SAs, simplex SPs)

Status & Open Issues

- original paper & running code presented at IWSSC‘07
  - encoder: module for uspace ULE generator (Linux 2.6.18)
  - decoder: kernel module for Linux DVB stack (Linux 2.6.18), trivial SP setup via configfs virtual filesystem interface
- identified issues:
  - identity protection + unicast SA: passive attacker may use Sequence Number to link packets together
    - envisaged solution: use encrypted counter as IV for e.g. CBC mode, turn Sequence Number field into “SA dependent data”
  - efficiency of identity protection: (how) do we limit number of trail-decryptions on receiver side?

Future Work

- work item 1 – address identified issues
- work item 2 – key management:
  - may be done separately and independent from this draft
  - reuse/adapt existing MSEC protocols
- work item 3 – possible cooperation:
  - see how/if we can work together on a single proposal within the WG