IPDVB WG Meeting (IETF-66) - Montreal

draft-cruickshank-ipdvb-sec-req-02.txt

Security requirements for ULE

Authors: H. Cruickshank and S. Iyengar
(University of Surrey, UK); L. Duquerroy
(Alcatel Alenia Space, Toulouse, France) and
P. Pillai (University of Bradford)

Draft status - 1

- This draft provides security requirements for MPEG-2 transmission links using the Unidirectional Lightweight Encapsulation (ULE), based on:
  - RFC 4259 (ipdvb architecture)
  - RFC 4326 (ULE method)
- Motivation:
  - Ability to provide security by the MPEG-2 transmission operator in relation to controlling access to the service.
  - Capability to work with IP and non-IP packet formats
  - Protect of ULE Receiver identity within MPEG-2 transmission network.
  - In a case of ULE Receiver receiving many IP streams: the decryption can be performed based on destination L2 address or each IP flow.

Draft status - 2

- Threat scenarios:
  - Scenario 1: Monitoring (passive threat)
  - Scenario 2: Local hijacking of MPEG-TS multiplex
  - Scenario 3: Global hijacking of MPEG-TS multiplex
- Requirements for passive threats:
  - Data confidentiality against passive threats
  - Protect of ULE Receiver identity.
- Requirements for active threats:
  - ULE encapsulator source authentication and data integrity.

Draft status - 3

- General security requirements:
  - Decoupling of key management functions from ULE security extensions.
  - Flexible security granularity: encrypt per MAC address (unicats and multicast) or per IP flow.
  - ULE link security is an additional security mechanism to IP, transport, and application layer security, not a replacement.

Discussions on ipdvb mailing list

- George Gross: Identity hiding/protection; temporary MAC address transitions; group SA re-keying requirement; source authentication; 64-bit sequence numbers; protecting against traffic analysis, etc..
- Art Allison: ATSC security system (ATSC A/70A); encryption based on PIDs
- Christian Praehauser: CRC checks.
- Gorry: various.

UniS

Future plans

- Incorporate all comments to a new draft:
  - Hopefully this work will be adopted as work item for ipdvb WG
- Produce new draft within one week:
  - Mailing list discussions
- Complete this work for the next IETF meeting