IPDVB WG Meeting (IETF-72) - Dublin

draft-ietf-ipdvb-sec-req-08.txt

Security requirements for ULE

Authors: H. Cruickshank and (University of Surrey, UK); P. Pillai (University of Bradford); M. Noisternig University of Salzburg, Austria and S. Iyengar (Logica, UK)

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.

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
- Five security requirements have been identified:
  - Scenario1: Data confidentiality (Req 1) MUST be provided and protection of NPA addresses (Req 2) MAY be provided
  - Case 2: In addition to Case 1 requirements, new measures MAY be implemented for integrity protection and source authentication (Req 2, Req 3 and Req 5). In addition, sequence numbers (Req 4) MAY be used to protect against replay attacks.
  - Scenario 3: similar to scenario 2, but easier to detect
- Appendix A describes security framework building blocks.

UniS

Summary of Changes in draft v7 and v8

- Version 7:
  - Rephrased some sentences throughout the document
  - Updated section 4 to more clearly specify requirements
  - Modified text in appendix section A.2.2 to correctly specify security information within the database
- Version 8:
  - Fixed some editorial mistakes and updated the reference list
  - Described the interface definitions in section A.2 as examples rather than requirements
- The draft is currently in WGLC

UniS