Security Extension for Unidirectional Lightweight Encapsulation (ULE) Protocol

draft-noisternig-ipdvb-sec-ext-01

Michael Noisternig (University of Salzburg)
Prashant Pillai (University of Bradford)
Haitham Cruickshank (University of Surrey)

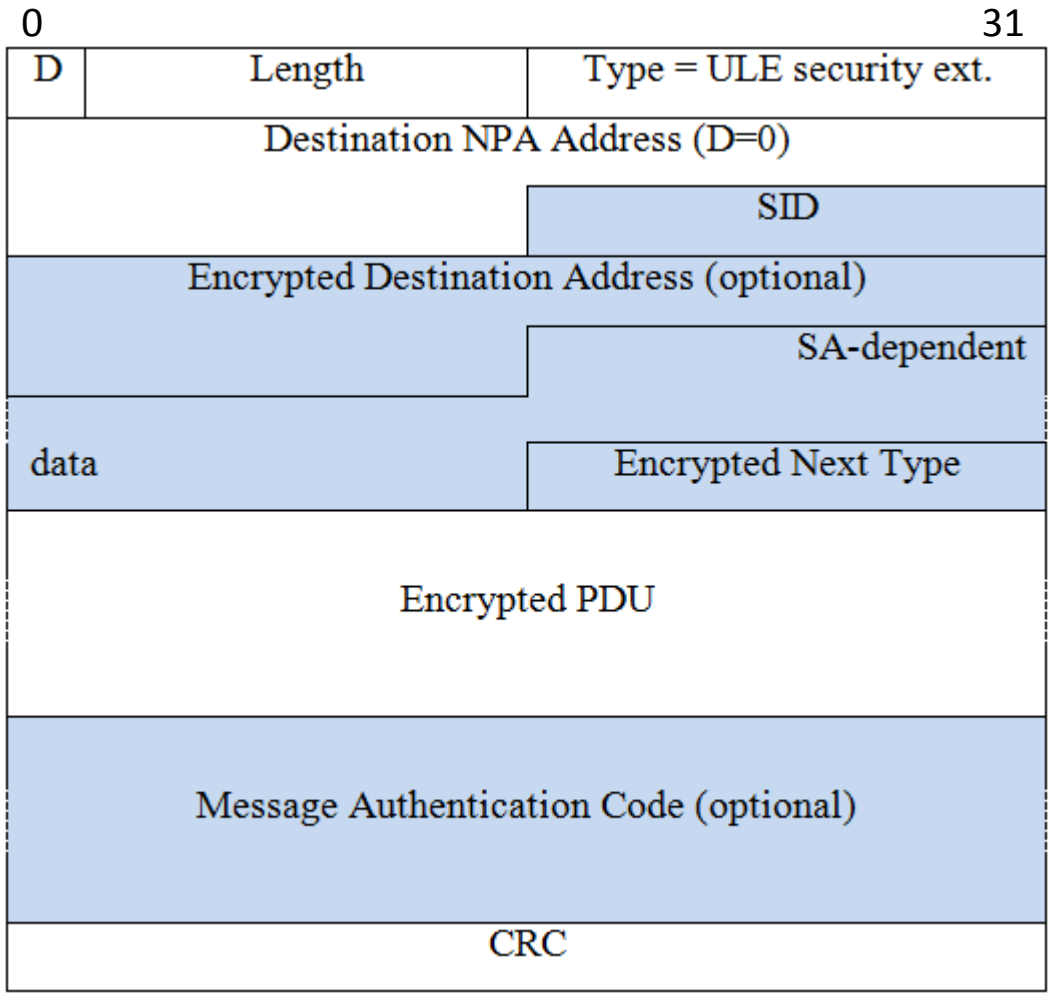
History

- builds on security requirements document RFC 5458 (March 2009)
  - why L2 security
  - threats & security requirements analysis
- based on individual drafts (July 2008)
  - draft-cruickshank-ipdvb-sec-05
  - draft-noisternig-ipdvb-ulesec-01
- joint conference papers (ICSSC´09, IWSSC´09)

Goals

- to provide security features identified in RFC 5458
- lightweight
  - low bandwidth and processing overhead
- flexible
  - support for different network configurations and security requirements, algorithm agility
- support for unidirectional links and multicast
- easily adaptable to GSE
  - aids transition of services to IP (“all-IP”)

New Extension Header Format



SA identifier

identity protection

encryption, replay protection *(sequence numbers, IVs, etc.)*

authentication, integrity protection *(MAC, [digital signature, TESLA, etc.])*

Extension Header Format Fields

- SID
  - 16 bits adequate for link-layer security
  - changed on re-keys
  - pre-defined set of SIDs to cycle through for unidirectional/multicast settings
- Identity protection/destination address encryption
  - possible in broadcast networks
  - effective (no false negatives, negligible chance of false positive)
- SA-dependent data field
  - no mandatory sequence numbers: not required in certain configurations (e.g., CBC encryption only, manual configurations), weakens identity protection (adversary may track sequence numbers and link to connection)
  - high flexibility (format defined via SA)
- MAC
  - realised as a trailer to ease processing (similar to CRC)

Transmitter/Receiver Processing

- based on IPsec approach
  - Security Association Database (SAD)
  - Security Policy Database (SPD)
  - SID (plus destination NPA, PID) for SA lookup
- extends longest-match approach for SA lookup
  - to prevent clashes between existing dynamically selected unicast SIDs and unilaterally assigned SIDs for multicast/ unidirectional links/shared SAs
  - if multicast address: longest-match search on (SID, destination NPA, PID) -> support for multicast groups
  - otherwise: longest-match search on (SID, PID) -> support for unidirectional links and single-sender shared SAs
- adds directionality to SPs
  - group communication, unidirectional links

Security Algorithms

- to be specified independently
  - allows proceeding/updating independently of this specification
- to be adapted from IPsec/MSEC specifications

Key Management

- manual keying via pre-shared keys
  - common for L2 security in managed networks
- key mgmt protocol to be specified independently
  - allows proceeding/updating independently of this specification
- MSEC/IPsec protocols may be adapted (e.g., GDOI, GSAKMP)
  - similar functionality wrt. SA lookup and databases
- existing L2 key management infrastructure may be re-used (e.g., DVB-RCS)
- support for unidirectional links

Security Issues

- identity protection issues
  - adversary may track increasing sequence number values
  - SID may resemble temporary address
- missing “true” source ID (PID) issues
  - auth PID or not?
  - sender ID for nonces/stream ciphers?
- other issues
  - stateful algorithms (manual keying)

Status

- joint specification
- implementation and interoperability test intended
- adaptable to GSE
- feedback desired
- **should this be adopted as a WG item?**