IPDVB WG Meeting (IETF-64) - Vancouver

draft-cruickshank-ipdvb-sec-req-00.txt

ULE security requirements

Authors: Haitham Cruickshank and Sunil Iyengar *(University of Surrey, UK);*
Stephane Combes and Laurence Duquerroy
(Alcatel Space, Toulouse, France)

Status of 63rd IETF meeting

- Presented draft-cruickshank-ipdvb-sec-00.txt
- Comments
  - The draft should first concentrate on a security requirements draft and then work on a solutions draft based on the requirements draft.
  - Missing HMACs for authentication was pointed out.
  - Pros and Cons of ULE security with respect to IPSec or underlying link layer security should be analysed.
  - Analyse impact of modifying/ insertion of SI tables and effects on security requirements in terms of threats –mailing list
- Written a new draft draft-cruickshank-ipdvb-req-00.txt, to take into the comments above and focus on requirements.

ULE Security

- A security analysis was provided in the I-D describing the ULE method [ULE] and the ipdvb architecture [ipdvb-arch].
- This draft extends that analysis
  - Derives the security requirements providing an overview of threat
  - ULE link security focuses on security between the Encapsulation Gateways (ULE source) and Receivers only.

ULE security requirements draft

- Threat Analysis
- Pros and Cons of IPSec and L2 security
- Pros and Cons of L2 security below ULE
- Motivation for ULE Security
- Security requirements for IP over MPEG2 networks

Security Requirements (1)

- Data confidentiality is the major requirement against passive threats (using encryption).
  - IPSec must be used in tunnel mode between ULE senders and receivers, which has more overheads.
- Optional protection of Layer 2 MAC/NPA address.
  - IPSec can not provide this service, however possible with L2 security.
- Layer L2 terminal authentication.
  - This will be part of the key management. It will be performed during the initial key exchange and authentication phase.
- For active threats ULE source authentication and data integrity are required
  - L2 data integrity/authentication is optional
  - Still important in environments in which several independent networks share a single transmission resource.

UniS

Security Requirements (2)

- End-to-end security (IPSec and TLS) and ULE link security should work in parallel without obstructing each other.
- Decoupling of ULE key management functions from ULE encryption.
- Compatibility with other networking functions: Other networking functions such as NAT/NAPT TCP acceleration can be used in a wireless DVB networks.

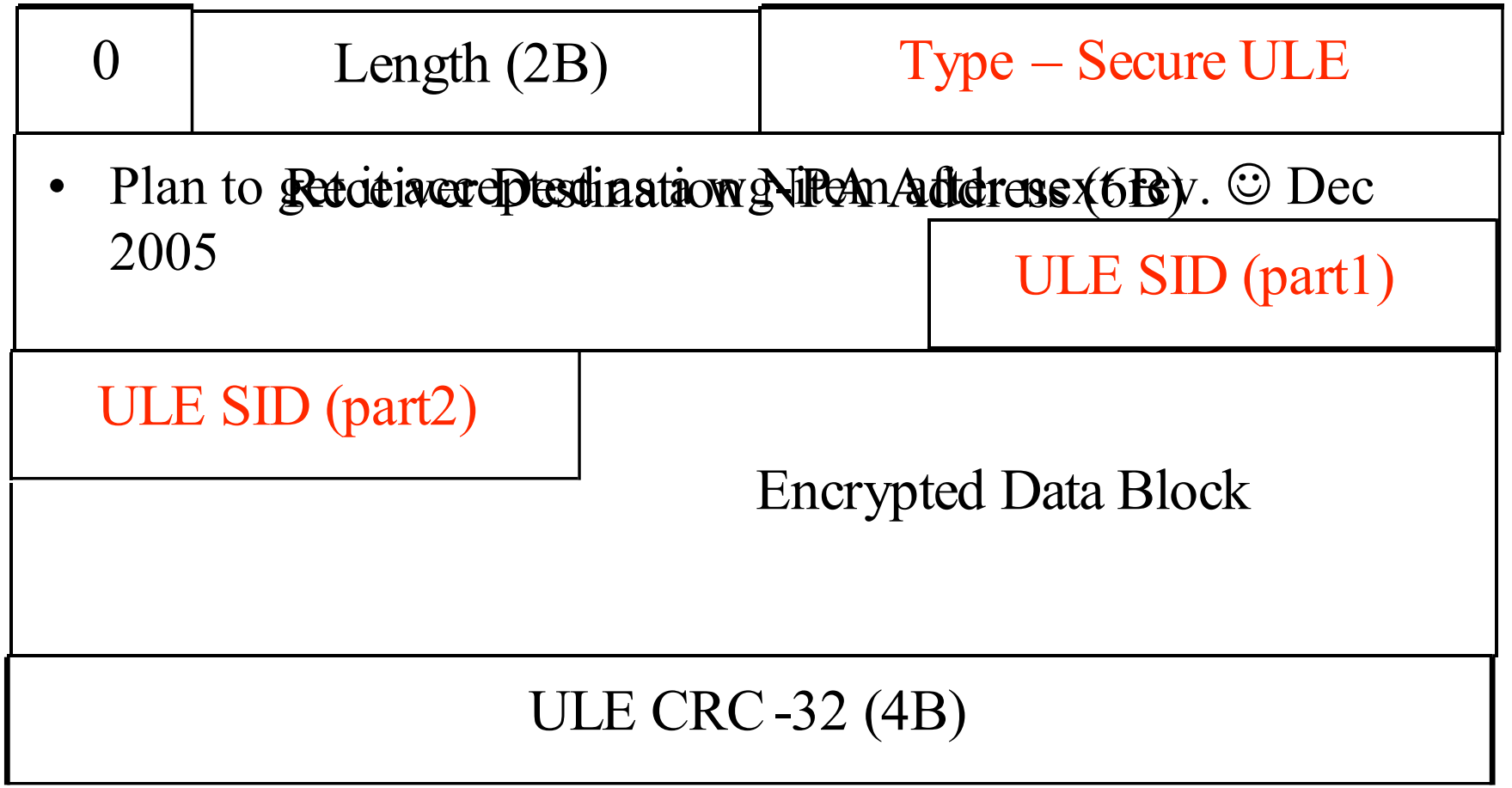
Goals of Link-Layer Security

- The protection of the complete ULE Protocol Data Unit (PDU) including IP addresses [RFC 3819].
- Ability to protect the identity of the Receiver within the MPEG-2 transmission network.
- Efficient protection of IP multicast over ULE links.

Topics to be addressed in next rev.

- Merits and demerits of IPSec,ULE and link layer security
- Authentication of the source (DVB Gateway)
- Vulnerabilities of the signalling
- Key Management Issues
- Working assumptions –in many systems physical security is assumed to be present when you buy into the package

Option 1 - SNDU Format for Encryption Header (D=0)



- Plan to get it accepted in w-IPA Adhoc ev. ☺ Dec 2005