IP-DVB WG Meeting (IETF-68) - Prague

draft-ipdvb-sec-01.txt
ULE Security Requirements

Presenter: Sunil Iyengar *University of Surrey, UK*

20/03/07

ULE Architecture Added

```
  +------------+                                  +------------+
  |  IP        |                                  |  IP        |
  |  End Host  |                                  |  End Host  |
  +-----+------+                                  +------------+
        |                                                ^
        +------------>+---------------+                  |
                      +  IP           |                  |
        +-------------+  Encapsulator |                  |
SI-Data |             +------+--------+                  |
+-------+-------+            |MPEG-2 TS Logical Channel  |
|  MPEG-2       |            |                           |
|  SI Tables    |            |                           |
+-------+-------+   ->+------+--------+                  |
        |          -->|  MPEG-2       |                . . .
        +------------>+  Multiplexor  |                  |
MPEG-2 TS             +------+--------+                  |
Logical Channel              |MPEG-2 TS Mux              |
                             |                           |
           Other    ->+------+--------+                  |
           MPEG-2  -->+  MPEG-2       |                  |
           TS     --->+  Multiplexor  |                  |
                 ---->+------+--------+                  |
                             |MPEG-2 TS Mux              |
                             |                           |
                      +------+--------+           +------+-----+
                      |Physical Layer |           |  MPEG-2    |
                      |Modulator      +---------->+  Receiver  |
                      +---------------+  MPEG-2   +------------+
                                         TS Mux
```

Security Requirements Added

- Data confidentiality is the major requirement.
- Protection of Layer 2 NPA address.
- Integrity protection and authentication of the ULE source is required against active attacks.
- Protection against replay attacks.
- Layer L2 ULE Source and Receiver authentication.

Security Scenarios

- Case 1: Monitoring (passive threat). Here the intruder monitors the ULE broadcasts to gain information about the ULE data and/or tracking the communicating parties identities (by monitoring the destination NPA).

- Case 2: Local hijacking of the MPEG-TS multiplex (active threat). Here an intruder is assumed to be sufficiently sophisticated to over-ride the original transmission from the ULE Encapsulation Gateway and deliver a modified version of the MPEG-TS transmission to a single ULE Receiver or a small group of Receivers (e.g. in a single company site).

- Case 3: Global hijacking of the MPEG-TS multiplex (active threat). Here we assume an intruder is very sophisticated and able to hijack the whole MPEG transmission multiplex.

- For both cases 2 and 3, there can be two sub cases:
  - Insider attacks i.e. active attacks from adversaries in the known of secret material.
  - Outsider attacks i.e. active attacks from outside of a virtual private network.

Security Scenarios Requirements

Case 1: Data confidentiality MUST be provided to prevent monitoring of the ULE data (such as user information and IP addresses). Protection of NPA addresses MUST be provided to prevent tracking ULE Receivers and their communications.

Case 2: In addition to case 1 requirements, new measures need to be implemented such as authentication schemes using Message Authentication Codes, digital signatures or TESLA [RFC4082] and using sequence numbers to prevent replay attacks in terms of insider attacks. In terms of outsider attacks group authentication using Message Authentication Codes should provide the same level of security. However, scenario 2 threats apply only in specific service cases and therefore source authentication and protection against replay attacks are OPTIONAL.

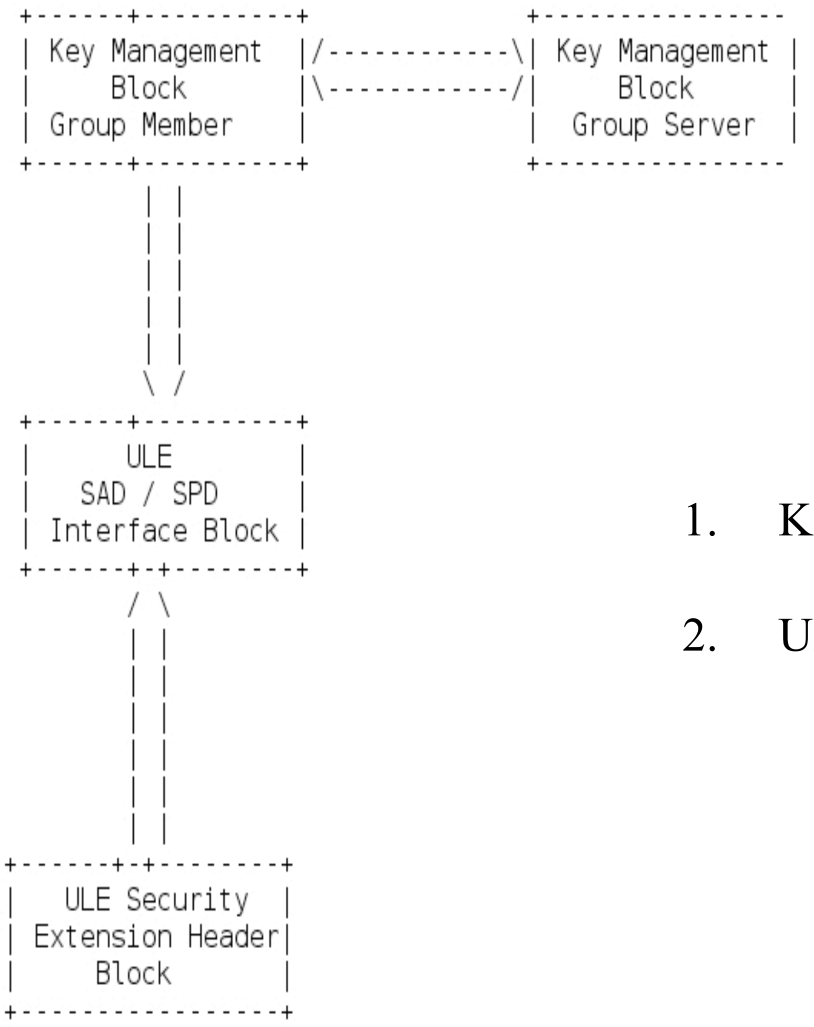
Case 3: The requirements here are similar to Case 2. In addition, intrusion detection is also desirable by the MPEG-2 network operator.

Revision History

- Working Group Draft revisions
  - Fixed editorial mistakes and ID style for WG adoption.
  - Major comments and suggestions (Michael Noistering) regarding authentication and integrity assurance. He also suggested that the threat scenarios section 3.2 should be expanded.
  - Elaborate the impact of threats for IP as opposed to Layer 2 (Gorry Fairhurst)
  - Algorithm Agility added as a requirement (gorry)

  - Fixed editorial mistakes and added some changes as pointed out by Knut (ESA) and added an appendix which shows the framework for securing the ULE network.

ULE Security Framework



```
+------+----------+        +----------------
| Key Management  |/-----------\| Key Management |
|     Block       |\-----------/|     Block      |
| Group Member    |             |  Group Server  |
+------+----------+        +----------------
          | |
          | |
          | |
          | |
          | |
          \ /
+------+----------+
|      ULE        |
|   SAD / SPD     |
| Interface Block |
+------+-+--------+
         / \
         | |
         | |
         | |
         | |
         | |
         | |
+------+-+--------+
|  ULE Security   |
| Extension Header|
|      Block      |
+-----------------+
```

Interfaces

1. Key management <-> ULE Security databases
2. ULE Security databases <-> ULE interfaces

Key Management Block

- This key management framework is responsible for user authentication, access control, and Security Association negotiation (which include the negotiations of the security algorithms to be used and the generation of the different session keys as well as policy material).

- This Key management framework can be either automated or manual.

- Hence Key management client entity will be present in all ULE receivers as well as ULE sources. In some cases the ULE source could also be the Key Server Entity.

- Existing key management protocols like GSAKMP, GDOI may be used or manual insertion of keying material can also be deployed.

ULE Security Block

- A new security extension header for the ULE protocol is required to provide the security features of data confidentiality, data integrity, data authentication and mechanisms to prevent replay attacks. Security keying material will be used for the different security algorithms (for encryption/decryption, MAC generation, etc.), which are used to meet the security requirements.

- This block will use the keying material and policy information from the ULE security database block on the ULE payload to generate the secure ULE extension Header or to decipher the secure ULE extension header to get the ULE payload.

- There could be other extension headers placed before or after the ULE Security Header extension

ULE Databases

- There needs to be two databases:
  - ULE-SAD: ULE Secure Association Database contains all the Security Associations that are currently established with different ULE peers.
  - ULE-SPD: ULE Secure Policy Database contains the policies as defined by the system manager. Those policies describe the security services that must be enforced.
- The design of these two databases will be based on IPSec databases as defined in RFC4301 [RFC4301].

Revision Future

- Fix editorial mistakes and added some changes as pointed out by Knut (ESA).
- Change WG draft status to INFO

- Sections to be updates:
  - Security Requirements
  - Appendix

- This revision should be ready by end of March 2007.

Conclusions

- Since most of the comments on the mailing list have been addressed Would like to request this draft to be adopted for IESG evaluation
- The next step would be to design the security extension and the interface documents as described in the framework as separate drafts.
- Not part of current charter but would like to continue input to the IPDVB group with guidance from the MSEC group ??
- Plan to have a working prototype based on our initial work in June.