

# Security requirements for IP over Satellite DVB networks

H. Cruickshank<sup>1</sup>, S. Iyengar<sup>1</sup>, S. Combes<sup>2</sup>, L. Duquerroy<sup>2</sup>, G. Fairhurst<sup>3</sup> and M. Mazzella<sup>1</sup>

**Abstract**— Security of data is becoming an important issue to operators and users of satellite networks. This paper analyses a set of threats and security requirements for IP over satellites with the focus on IPv6 using DVB transmission. It also defines the requirements for satellite DVB security and states the motivation for link security as a part of the encapsulation layer.

**Index Terms**— Security, Conditional Access, multicast, DVB-S, DVB-RCS, ipdvb.

## I. INTRODUCTION

This work started during the preparations for the IST project called SATSIX (Satellite-based communications systems within IPv6). SATSIX [1] will implement innovative concepts and cost-effective solutions for broadband satellite systems and services. The project promotes the introduction of the IPv6 protocol into satellite-based communication systems. A prime focus for these systems will be service platforms built upon the sound basis established by the European Digital Video Broadcast standards for satellite systems (DVB-RCS [RCS], and DVB-S2 [S2]).

DVB utilises the ISO MPEG-2 Transport Stream (TS), which has been widely accepted, not only for providing digital TV services, but also as a subnetwork technology for building IP network. In terms of the IP service, the DVB standards are neither optimal nor complete. The forward link of DVB-RCS (utilising DVB-S [2]) currently specifies MPEG-2 packetisation, whilst the return link uses optional MPEG-2 or ATM packetisation. Work is in progress to extend the forward link to utilise the new DVB-S.2 standard that supports advanced physical layers with the opportunity to utilise adaptive coding/modulation. Both DVB-S and DVB-S.2 can support the MPEG-TS, but the latter also provides an opportunity to define a new encapsulation method tailored to the IP-service and designed to offer improved performance when used in combination with adaptive coding/modulation.

The DVB-RCS standard defines basic interoperability between DVB-RCS systems and adaptation to various higher layers via Multi-Protocol Encapsulation (MPE) at the link-

layer [MPE]. Additional functions at and above the link-layer 2 need to be specified to fully adapt IP services (e.g. QoS, security, multicast) to DVB-RCS (including satellites with OBP switching), although this paper is concerned only with security issues.

Recent work within the IETF has led to standardisation of an alternative encapsulation layer, the Unidirectional Lightweight Encapsulation (ULE) [6]. ULE specifies an encapsulation format that may natively transport IPv4 and IPv6 Datagrams, bridged Ethernet frames and other network protocol packets (generally referred to as Subnetwork Data Units, SNDUs) directly over MPEG-2 as TS Private Data. ULE also supports an extension format that allows it to carry additional header information to assist in network/Receiver processing.

## II. SECURITY REQUIREMENTS

The EC SATSIX Project is defining a set of security requirements for the satellite DVB-RCS networks, a link-layer security protocol and the interworking of the SatIPSec solution and link-layer security. This work is directly related to the on-going standardisation work of the IETF ipdvb WG for MPEG2-transmission networks and the standardisation activities for satellite systems within ETSI/BSM.

Key characteristics of MPEG-2/DVB transmission networks are that they may provide link-level broadcast, and that many supported applications require access to a very large number of subnetwork nodes, i.e. Receiver terminals [6]. The security requirements for a link concern the link-layer path between the Encapsulation Gateways (ULE source) and the Receiver terminal(s). The ipdvb architecture [6] describes several components that may also be present in this path including TS multiplexors (including re-multiplexors), and modulators. In the case of DVB-RCS this may also include regenerative satellite payloads.

The majority of MPEG-2/DVB transmission networks are wireless, and hence are bandwidth-limited, encapsulation protocols must therefore add minimal overhead to ensure good link efficiency while providing adequate security services. They also need to be simple to minimize processing, robust to errors/loss of packets and address the security threats, while remaining applicable to a wide range of services.

SatIPSec is a network-layer security solution that was

<sup>1</sup> Centre for Communication Systems Research, University of Surrey, Guildford, UK

<sup>2</sup> Telecom Satellite Systems, Alcatel-Alenia Space, Toulouse, France

<sup>3</sup> Department of Engineering, University of Aberdeen, UK

developed in the IST SatIP6 project [satip6]. It is a method that may secure unicast and multicast satellite transmissions on the forward and return links, in DVB-RCS star and mesh topologies, based on IPsec [ipsec]. There are two main entities: the SatIPSec client and SatIPSec Group Controller & Key Server (GCKS). In SATSIX, this will be adapted to provide link-layer security suited to link using ULE. Thus requires one SatIPSec client module to be integrated in each encapsulation gateway and receiver. The GCKS, which configures SatIPSec clients, is integrated in the DVB-RCS gateway (GW) or Network Control Centre (NCC).

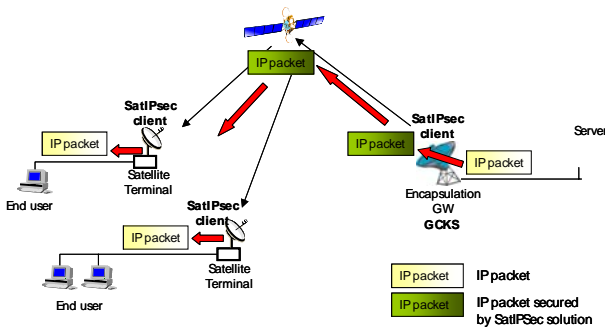


Figure 1. Protection of satellite IP transmissions by SatIPSec solution.

### III. THREAT ANALYSIS

When the MPEG-2 transmission network is not using a wire-line network, the normal security issues relating to the use of wireless links for transport of Internet traffic should be considered. An initial analysis of the security requirements in MPEG-2 transmission networks has been provided in the security consideration section of [3]. This recommends that any new encapsulation defined by the IETF should allow Transport Stream encryption and also support optional link level encryption / authentication of the SNDU payload. In the remainder of this section, we extend this threat analysis:

The simplest type of network threat is a passive threat. Passive attacks include eavesdropping or monitoring of transmissions, with a goal to obtain information that is being transmitted. In broadcast networks (especially those utilising widely available low-cost physical layer interfaces, such as DVB) passive threats are considered the major threat. An example is an intruder monitoring the transmission to extract traffic communicated between IP hosts. Another example is an intruder obtaining information about the communication parties by monitoring the level of activity at the link-layer associated with specific MAC/NPA addresses. Through this, an intruder could gain traffic statistics associated with a particular communicating party (e.g. the volume and timing of their traffic). This is a well-known security issue, however the ease of interception makes this more problematic in broadcast networks such as DVB transmission networks.

Active threats (or attacks) require an intruder to inject/modify information into the received bitstream. These are, in general, more difficult to implement successfully than

passive threats, and usually require more sophisticated resources. Examples of active attacks are:

- Masquerading: where an entity pretends to be a different entity. This includes masquerading other users and subnetwork control plane messages.
- Modification of messages in an unauthorised manner.
- Repudiation: Repudiation of origin occurs when a party denies being the originator of a message and repudiation of destination occurs when a party denies the reception of a message. However, this is an end-to-end application layer issue and does not apply to link-layer communications.
- Replay attacks: When an intruder sends additional copies of old (authenticated) messages to the Receiver.
- Denial of service attacks: When an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions.

Active threats such as replay masquerading, modification of messages and injecting IP packet attacks are major security concerns for the Internet community operating at the network-layer. As such, Steve Bellovin [8] describes several of these attacks. The defence against such attacks is data integrity using cryptographic techniques and sequence numbers.

An active attack against a broadcast network requires access to a transmitter that can create a Stream that (partially) replaces the intended Stream at the Receiver. This threat could be realised by access to the Hub station of a satellite network (which is normally protected by other security measures), access to a valid/compromised user terminal, or transmission from a local transmitter that directly injects data into the receive antenna of another user. Although such attacks such are more difficult at the link than network layers, attacks on individual ULE Receivers are possible and could pass unnoticed by the satellite network operators and/or ISPs.

Active threats need careful consideration in the context of MPEG-2 transmission links. To counter an active threat requires source authentication. In an IP network the source and destination are the security tunnel end-point and/or the end-host themselves. A typical integrity check, e.g. MD5, adds 20 bytes and a typical sequence numbering requires 4 bytes. At the link-layer, the source is an Encapsulation Gateway and the Receiver(s) are the destination(s). The ULE method is a lightweight protocol and the security method needs to be careful not to turn this into a heavyweight protocol by addition of security authentication. Therefore new lightweight data integrity methods or procedures are needed, for example to authenticate the Stream rather than individual SNDUs.

#### IV. SECURITY REQUIREMENTS FOR IP OVER MPEG-2 TS

From the above analysis, the following security requirements can be derived:

- End-to-end security (such as IPsec and TLS) and ULE link security should work in parallel without obstructing each other. Each has its own role.
- Data confidentiality is the major requirement against passive threats (using encryption). L2 encryption or L3 (IPsec) encryption can satisfy this requirement. However when IPsec is not already used end-to-end, IPsec would need to be used in tunnel mode between ULE gateways and receivers, which introduces additional protocol overhead.
- Optional protection of Link-Layer MAC/NPA address. This is needed in the broadcast networks to prevent an intruder gaining information through knowledge of the identity of the communicating parties and their traffic characteristics. IPsec can not provide this service at the network layer, however it is possible with link security systems.
- Link-layer terminal authentication is a part of the key management and will be performed during the initial key exchange and authentication phase.
- ULE authentication and data integrity checks are required to defeat active threats are required. Sequence numbers are required to prevent replay attacks. Although L2 data integrity/authentication is optional, it is still important in environments in which several independent networks share a single transmission resource.
- The integrity and authentication of the control and management messages used by the network also needs to be considered, since these are required for proper operation of the system.
- Decoupling of ULE key management functions from ULE encryption will allow the independent definition of these subsystems. Suitable approaches include re-use of existing security management systems (e.g. GSAKMP [12] and GDOI [13] from the IPsec architecture other systems such as DVB-RCS [9] and/or the development of new systems, as required.

Other general requirements are:

- Protection of the management system and the infrastructure from unauthorised people. ULE encryption will provide partial protection through key management procedures and data encryption.
- Operational issues: The possible large geographic coverage of a broadcast transmission network may require delivery of data to many different countries that may have different security legislation (related to authorized encryption algorithms and the length of keys). Therefore to offer flexibility to operators,

the security system should permit a range of security parameters during the negotiation phase . In ULE security, the choice of such algorithms will be decided by the key management system in use.

- Compatibility with other networking functions: Other networking functions such as NAT/NAPT (Network Address Translation) or TCP acceleration are often used in a wireless DVB network. The ULE security solution should be compatible with such midbox functions.
- Traceability (such as intrusion detection systems) to monitor transmission network (e.g. using log files to record the activities on the network). This is out of scope for ULE security.

#### V. IPSEC AND MPEG-2 TRANSMISSION NETWORKS

The Security Architecture for the Internet Protocol [15] describes security services for traffic at the IP layer. That architecture primarily defines services for Internet Protocol (IP) unicast packets, as well as manually configured IP multicast packets.

IPsec supports two modes of use: transport mode and tunnel mode. In transport mode, AH and ESP provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to the tunnelled IP packets. In both modes, data integrity is provided and in addition, ESP also provides the data privacy service.

IP Multicast is considered a major service over MPEG-2 Transmission Networks. The msec working group of the IETF [14] have been defining IPsec extensions for multicast [15] that define how IP multicast may be used within the IPsec security architecture for packets with a multicast address in the IP destination field.

##### A. End-to-End security

IPsec in transport mode can provide end-to-end security between the pairs of end-hosts using an IP network. This mode of operation is not compatible with the use of NAT/NAT-PT and other midbox functions (including protocol accelerators), and is not common in the currently deployed IPv4 Internet, it has however been suggested as an important service for IPv6. The use of end-to-end security is transparent to the transmission links and has no additional impact on their operation.

##### B. Tunnel mode use of IPsec for multicast

In the context of MPEG-2 transmission, if IPsec is used to secure the satellite link, then the ULE gateways and Receivers are equivalent to security gateways in IPsec. A security gateway implementation of IPsec using the multicast extensions will use tunnel mode to encapsulate the IP packets.

IPsec tunnel mode has two challenges: First, if the destination of an IP multicast packet is changed it will no longer be properly routed. Secondly, IP multicast routing protocols also typically create multicast distribution trees

based on the source address. An IPsec security gateway that changes the source address of an IP multicast packet, again this will cause multicast routing problems. The proposed multicast extensions to IPsec [14] define a way for retaining both the IP source and destination addresses of the inner IP header to allow IP multicast routing protocols to route the packet irrespective of the packet being IPsec protected. This method of tunnel mode is known as “tunnel mode with address preservation”.

### C. IPsec and L2 security

If IPsec is used by an operator to secure ULE links, then it must be used in tunnel mode. Such usage has the following disadvantages:

- There is a need to protect the identity of ULE encapsulator/Receivers over the ULE broadcast medium; IPsec can not provide this service.
- There is additional overhead associated with using IPsec in tunnel mode, i.e. IPv4 or IPv6 header
- Multicast is a major service. The current IPsec specifications only define a pairwise tunnel between two IPsec devices with manual keying. Work in progress [14] is defining the functions needed for multicast and tunnel mode with address preservation. In the ULE link context, in addition to the IPsec tunnelling overheads, the source and destination address preservation means that these IP addresses are broadcast in the clear. This can prevent identity hiding over the transmission link. Multicast data may also [14] be sent through a service provider network, and encapsulated under a different IP multicast address while in a provider network (e.g. the source address of the outside IP header could be set to that of the DVB gateway).

## VI. MOTIVATION FOR ULE LINK LAYER SECURITY

The threat analysis and security requirements described in sections 3 and 4 demonstrate a need to provide link-layer security in MPEG-2 transmission networks employing ULE. Particularly when network-layer and transport-layer security (e.g. IPsec, TLS) alone are not sufficient.

ULE link security is considered an additional security mechanism to IPsec, and end-to-end methods at the transport, and application layers, not a replacement. While functions resemble those of IPsec, it provides additional link confidentiality and Receiver identity hiding over the transmission link. There is no direct interaction between IPsec and the ULE security system.

Since link-layer security acts below the network-layer, it may be used in any combination with midboxes that require the ability to inspect and modify the packets sent over the link, e.g. performing Virtual Private Network (VPN) functions, Network Address Translation (NAT), TCP acceleration (TCP-PEP). It also does not preclude the use of IPsec.

In common with other security methods, link-layer security

also requires a key distribution and management framework. A suitable method should have the ability to use a range of cryptographic algorithms, and enable re-use of established encryption libraries. In this respect, ULE may use and benefit from IETF key management protocols designed to operate with IPsec, such as the MSEC GSAKMP [12] and GDOI [13]. Link-layer security may also utilize pre-placed keys and other key management architectures (e.g. common key management to DVB-RCS).

### A. Link security below the Encapsulation layer

One method to provide link-layer security is at the MPEG-TS level (below ULE). MPEG-TS encryption encrypts all TS Packets sent over a particular stream (i.e. with a specific PID value). However, the common use of the MPEG-TS multiplexes several IP streams and/or other MPEG services using a common Stream (i.e. PID value). In this method, all the multiplexed traffic will share the same security keys. This has a number of disadvantages:

- Each ULE Receiver needs to decrypt some MPEG-TS packets that it does not finally use/forward. When software-based receivers and/or cryptos are used, this additional traffic represents a significant processing burden.
- A ULE Receiver will be able to see all traffic destined to other ULE Receivers sharing the common key.
- If the key is compromised, then this will impact all ULE Receivers that share the key.

### B. Link security as a part of the Encapsulation layer

Another method is to provide Link-layer security within the encapsulation layer, e.g. using MPE or as a ULE Header Extension function.

In some current encapsulation methods, e.g. MPE [9], encryption of the MAC address requires each Receiver to decrypt all encrypted data sent using a TS Logical Channel (PID), before it can then filter the PDUs that match the set of MAC/NPA addresses that the Receiver wishes to receive, therefore encryption of the MPE MAC address is not permitted in such systems.

The main advantages of ULE link security are:

- The protection of the complete ULE Protocol Data Unit (PDU) including IP addresses, and where appropriate to validate the associated MAC/NPA address to which the PDU is bound.
- Ability to protect (hide) the identity of the Receiver within the transmission network.
- ULE supports a range of packet formats, and the encryption method may also therefore be applicable to services that were not IP-based (although the use of IPsec key management may

still be desirable).

- Efficient protection of IP multicast over ULE

The threat analysis in section 4, showed that protection of ULE link from eavesdropping and ULE Receiver identity hiding are major requirements. Such requirements can be met using ULE link encryption.

If support is required for non-IP traffic, then the IPsec architecture would need to be extended, since IPsec relies on port numbers, etc to define the flows within the Security Policy Database (SPD). Equivalent access points would need to be defined for other protocol families. The cost and complexity of such an approach have not been evaluated, but could form future research, should a ULE security mechanism be defined.

The ULE security system should be incremental and provide ULE link encryption as a basic service. A method that utilises a Mandatory ULE Extension Header [ULE] has therefore been proposed [SEC-REQ]. This method also provides considerable flexibility when used with other extension mechanisms, allowing protocol control information to be associated with a PDU in either the encrypted or unencrypted part of a SNDU. The method is also expected to be complementary to future extensions, such as support for link QoS and/or link header compression, if and when such extensions are defined.

In the context of active threats, ULE authentication is also required, and lightweight methods need to be found (compared to IPsec, where authentication overhead is added to each individual IP packet). Additional services such as data integrity and replay prevention (based on sequence number) should only be provided where needed, and where the associated overhead/processing cost can be justified.

## VII. CONCLUSION

This paper analyses a set of threats and security requirements. It also defines the requirements for ULE security and states the motivation for Link security as a part of the encapsulation layer. In summary, there is a need for L2 encryption, ULE Receiver identity hiding, L2 source authentications and protection against insertion of other data into a ULE Stream. The paper focuses only on links utilising the MPEG-2 Transport Stream, but common security methods may also in future be defined that also apply to other DVB-based transmission systems, such as the Generic Stream offered by DVB-S2.

## ACKNOWLEDGEMENT

This work was supported by the EU Information Society Technologies SATSIX project, IST-2-26950. The authors gratefully acknowledge the JA2350 activity of the EU Information Society Technologies SatNEx Project which assisted in definition of the security threats.

## REFERENCES

- [1] SATSIX web address ?
- [2] EN 301 421,"Digital Video Broadcasting (DVB); Modulation and Coding for DBS satellite systems at 11/12 GHz, European Telecommunications Standards Institute (ETSI).
- [3] EN 301 790, "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems", European Telecommunications Standards Institute (ETSI).
- [4] EN 302 307, "Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications", European Telecommunication Standards Institute (ETSI).
- [5] EN 301 192 Specifications for Data Broadcasting, European Telecommunications Standards Institute (ETSI).
- [6] Fairhurst, G. and B. Collini-Nocker, "Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)", RFC 4326, December 2005.
- [7] M-J Montpetit, G. Fairhurst, H.D. Clausen, B. Collini-Nocker, H. Linder, (2005) A Framework for Transmission of IP Datagrams over MPEG-2 Networks, IETF RFC 4259, December 20055.
- [8] [Bellare] Bellare, S., "Problem Area for the IP Security Protocols", Computer Communications Review 2:19, pp. 32-48, April 1989. <http://www.cs.columbia.edu/~smb/>.
- [9] [ETSI-DVBRCS] "Digital Video Broadcasting (DVB) -- interaction channel for satellite distribution systems", ETSI EN 301 790 V1.4.1 (2005-04)
- [10] <http://www.ietf.org/html.charters/wg-dir.html#Security%20Area>. RFCs 2401, 2402 and 2406
- [11] [msec] <http://www.ietf.org/html.charters/msec-charter.html>
- [12] [msec-gsakmp] H Harney (SPARTA ), et al, "GSAKMP: Group Secure Association Group Management Protocol", <draft-ietf-msec-gsakmp-sec-10.txt>, IETF Work in Progress.
- [13] [msec-gdoi], RFC 3547] M. Baugher , et al, "GDOI: The Group Domain of Interpretation" RFC 3547, IETF.
- [14] [msec-ipsec-ext] Weis B., et al, "Multicast Extensions to the Security Architecture for the Internet", <draft-ietf-msec-ipsec-extensions-00.txt>, IETF Work in Progress.
- [15] [RFC2401BIS] Kent, S. and Seo K., "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-06.txt, IETF work-in-progress, March, 2005.
- [16] L. Duquerroy, S. Josset, O. Alphand, P. Berthou and T. Gayraud "SatIPSec : an optimized solution for securing multicast and unicast satellite transmissions", 22<sup>nd</sup> AIAA International Communications Satellite Systems Conference, Monterey, May 2004.
- [17] H. Cruickshank, S. Iyenger, S. Combes, L. Duquerroy "Security requirements for the Unidirectional Lightweight Encapsulation (ULE) protocol", IETF work-in-progress, draft-cruickshank-ipdvb-sec-req-xx.txt, 2005.