Internet Engineering Task Force
Internet Draft
draft-cruickshank-ipdvb-sec-req-04.txt

H.Cruickshank
S. Iyengar
University of Surrey, UK
L. Duquerroy
Alcatel Alenia Space, France
P. Pillai
University of Bradford, UK

Expires: April 4, 2007

Category: Internet Draft

October 14, 2006

Security requirements for the Unidirectional Lightweight Encapsulation (ULE) protocol draft-cruickshank-ipdvb-sec-req-04.txt

Status of this Draft

Abstract

The MPEG-2 standard defined by ISO 13818-1 [ISO-MPEG2] supports a range of transmission methods for a range of services. This document provides a threat analysis and derives the security requirements when using the Transport Stream, TS, to support an Internet network-layer using Unidirectional Lightweight Encapsulation (ULE) [RFC4326]. The

document also provides the motivation for link-level security for a ULE Stream. A ULE Stream may be used to send IPv4 packets, IPv6 packets, and other Protocol Data Units (PDUs) to an arbitrarily large number of Receivers supporting unicast and/or multicast transmission.

Table of Contents

1. Introduction

The MPEG-2 Transport Stream (TS) has been widely accepted not only for providing digital TV services, but also as a subnetwork technology for building IP networks. RFC 4326 [RFC4326] describes the Unidirectional Lightweight Encapsulation (ULE) mechanism for the transport of IPv4 and IPv6 Datagrams and other network protocol packets directly over the ISO MPEG-2 Transport Stream as TS Private Data. ULE specifies a base encapsulation format and supports an extension format that allows it to carry additional header information to assist in network/Receiver processing. The encapsulation satisfies the design and architectural requirement for a lightweight encapsulation defined in RFC 4259 [RFC4259].

Section 3.1 of RFC 4259 presents several topological scenarios for MPEG-2 Transmission Networks. A summary of these scenarios are presented below (for full detail, please refer to RFC 4259).

1. Broadcast TV and Radio Delivery.

2. Broadcast Networks used as an ISP. This resembles to scenario 1, but includes the provision of IP services providing access to the public Internet.

3. Unidirectional Star IP Scenario. It utilizes a Hub station to provide a data network delivering a common bit stream to typically medium-sized groups of Receivers.

4. Datacast Overlay. It employs MPEG-2 physical and link layers to provide additional connectivity such as unidirectional multicast to supplement an existing IP-based Internet service.

5. Point-to-Point Links.

6. Two-Way IP Networks. This can be typically satellite-based and star-based utilising a Hub station to deliver a common bit stream to medium- sized groups of receivers. A bidirectional service is provided over a common air-interface.

RFC 4259 states that ULE must be robust to errors and security threats. Security must also consider both unidirectional as well as bidirectional links for the scenarios mentioned above.

An initial analysis of the security requirements in MPEG-2 transmission networks is presented in the security considerations section of RFC 4259. For example, when such networks are not using a wireline network, the normal security issues relating to the use of wireless links for transport of Internet traffic should be considered [RFC3819].

The security considerations of RFC 4259 recommends that any new encapsulation defined by the IETF should allow Transport Stream encryption and should also support optional link-level authentication of the SNDU payload. In ULE [RFC4326], it is suggested that this may be provided in a flexible way using Extension Headers. This requires the definition of a mandatory header extension, but has the advantage that it decouples specification of the security functions from the encapsulation functions.

This document extends the above analysis and derives a detailed the security requirements for ULE in MPEG-2 transmission networks.

2. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

Other terms used in this document are defined below:

ATSC: Advanced Television Systems Committee. A framework and a set of associated standards for the transmission of video, audio, and data using the ISO MPEG-2 standard.

DVB: Digital Video Broadcast. A framework and set of associated standards published by the European Telecommunications Standards Institute (ETSI) for the transmission of video, audio, and data using the ISO MPEG-2 Standard [ISO-MPEG2].

Encapsulator: A network device that receives PDUs and formats these into Payload Units (known here as SNDUs) for output as a stream of TS Packets.

LLC: Logical Link Control [ISO-8802-2, IEEE-802.2]. A link-layer protocol defined by the IEEE 802 standard, which follows the Ethernet Medium Access Control Header.

MAC: Message Authentication Code.

MPE: Multiprotocol Encapsulation [ETSI-DAT]. A scheme that encapsulates PDUs, forming a DSM-CC Table Section. Each Section is sent in a series of TS Packets using a single TS Logical Channel.

MPEG-2: A set of standards specified by the Motion Picture Experts Group (MPEG) and standardized by the International Standards Organisation (ISO/IEC 13818-1) [ISO-MPEG2], and ITU-T (in H.222 [ITU-H222]).

NPA: Network Point of Attachment. In this document, refers to a 6-byte destination address (resembling an IEEE Medium Access Control address) within the MPEG-2 transmission network that is used to identify individual Receivers or groups of Receivers.

PDU: Protocol Data Unit. Examples of a PDU include Ethernet frames, IPv4 or IPv6 datagrams, and other network packets.

PID: Packet Identifier [ISO-MPEG2]. A 13-bit field carried in the header of TS Packets. This is used to identify the TS Logical Channel to which a TS Packet belongs [ISO-MPEG2]. The TS Packets

forming the parts of a Table Section, PES, or other Payload Unit must all carry the same PID value. The all-zeros PID 0x0000 as well as other PID values are reserved for specific PSI/SI Tables [ISO-MPEG2]. The all-ones PID value 0x1FFF indicates a Null TS Packet introduced to maintain a constant bit rate of a TS Multiplex. There is no required relationship between the PID values used for TS Logical Channels transmitted using different TS Multiplexes.

Receiver: Equipment that processes the signal from a TS Multiplex and performs filtering and forwarding of encapsulated PDUs to the network-layer service (or bridging module when operating at the link layer).

SI Table: Service Information Table [ISO-MPEG2]. In this document, this term describes a table that is defined by another standards body to convey information about the services carried in a TS Multiplex. A Table may consist of one or more Table Sections; however, all sections of a particular SI Table must be carried over a single TS Logical Channel [ISO-MPEG2].

SNDU: SubNetwork Data Unit. An encapsulated PDU sent as an MPEG-2 Payload Unit.

TS: Transport Stream [ISO-MPEG2], a method of transmission at the MPEG-2 level using TS Packets; it represents layer 2 of the ISO/OSI reference model. See also TS Logical Channel and TS Multiplex.

TS Multiplex: In this document, this term defines a set of MPEG-2 TS Logical Channels sent over a single lower-layer connection. This may be a common physical link (i.e., a transmission at a specified symbol rate, FEC setting, and transmission frequency) or an encapsulation provided by another protocol layer (e.g., Ethernet, or RTP over IP). The same TS Logical Channel may be repeated over more than one TS Multiplex (possibly associated with a different PID value) [RFC4259]; for example, to redistribute the same multicast content to two terrestrial TV transmission cells.

TS Packet: A fixed-length 188B unit of data sent over a TS Multiplex [ISO-MPEG2]. Each TS Packet carries a 4B header, plus optional overhead including an Adaptation Field, encryption details, and time stamp information to synchronise a set of related TS Logical Channels.

3. Threat Analysis

3.1. System Components

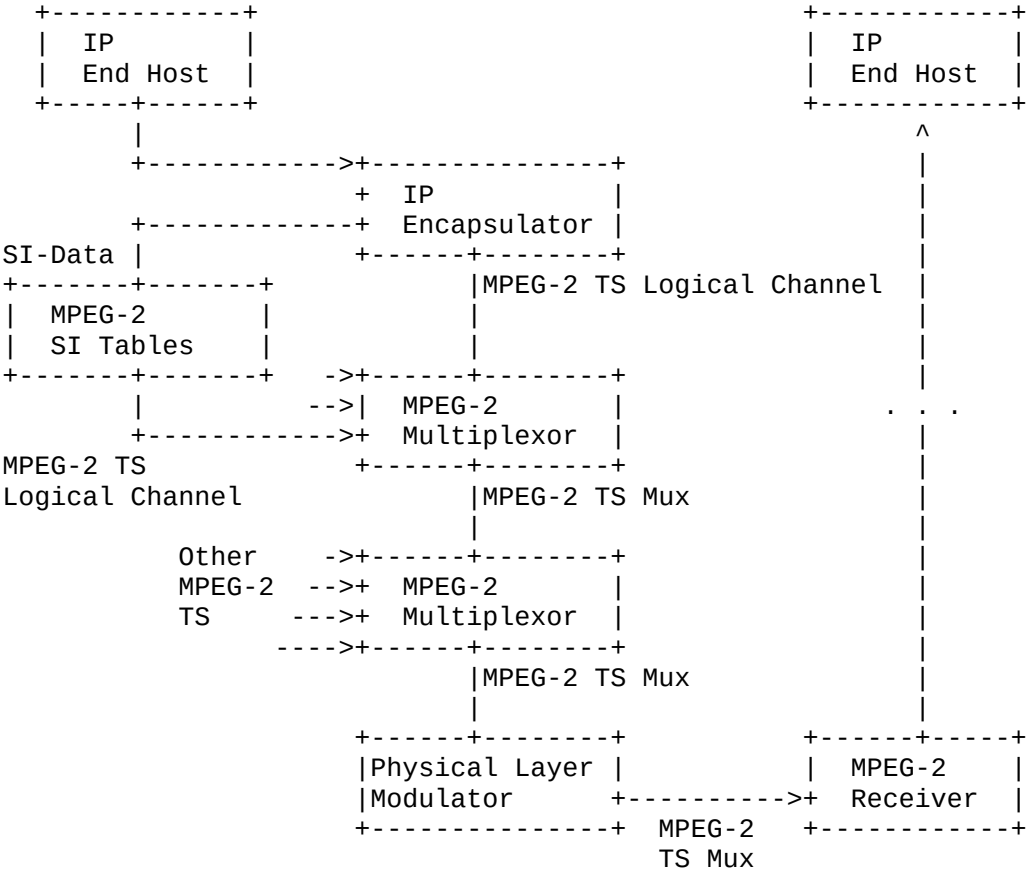

Figure 1 :An example configuration for a unidirectional Service for IP transport over MPEG-2 [RFC4259].

As shown in Figure 1 (in section 3.3 of [RFC4259]), there are several entities within the MPEG-2 transmission network architecture. These include:

- ULE Encapsulation Gateways (or Encapsulator or ULE source)
- SI-Table signalling generator (input to the multiplexor)

- Receivers
- TS multiplexers (including re-multiplexers)
- Modulators

In an MPEG-2 network a set of signalling messages [ID-AR] may need to be broadcast (e.g. by an Encapsulation Gateway) or other device to form the L2 control plane. Examples of signalling messages include the Program Association Table (PAT), Program Map Table (PMT) and Network Information Table (NIT). In existing MPEG-2 transmission networks, these messages are broadcasted in the clear (no encryption or integrity checks). The integrity of these messages is important for correct working of the ULE network. However, securing these messages is out of scope for ULE security, because these messages are not normally encapsulated with the ULE method.

ULE link security focuses only on the security between the ULE Encapsulation Gateway (ULE source) and the Receiver. Securing the ULE source and receivers eliminates the need to consider security issues regarding the remaining system components, such as multiplexers, re-multiplexers and modulators.

In a MPEG-2 TS transmission network, the originating source of TS Packets is either a L2 interface device (media encoder, encapsulation gateway, etc) or a L2 network device (TS multiplexer, etc). These devices may, but do not necessarily, have an associated IP address. In the case of an encapsulation gateway (e.g. ULE sender), the device may operate at L2 or L3, and is not normally the originator of an IP traffic flow, and usually the IP source address of the packets that it forwards do not correspond to an IP address associated with the device. When authentication of the IP source is required this must be provided by IPsec, TLS, etc. operating at a higher layer.

The TS Packets are carried to the Receiver over a physical layer that usually includes Forward Error Correction coding that interleaves the bytes of several consecutive, but unrelated, TS Packets. FEC coding and synchronisation processing makes injection of single TS Packets very difficult. Replacement of a sequence of packets is also difficult, but possible (see section 3.2).

A Receiver in a MPEG-2 TS transmission network needs to identify a TS Logical Channel (or MPEG-2 Elementary Stream) to reassemble the fragments of PDUs sent by a L2 source [RFC4259]. In an MPEG-2 TS, this association is made via the Packet Identifier, PID [ISO-MPEG2]. At the sender, each source associates a locally unique set of PID values with each stream it originates. However, there is no required

relationship between the PID value used at the sender and that received at the Receiver. Network devices may re-number the PID values associated with one or more TS Logical Channels (e.g. ULE Streams) to prevent clashes at a multiplexer between input streams with the same PID carried on different input multiplexes (updating entries in the PMT [ISO-MPEG2], and other SI tables that reference the PID value). A device may also modify and/or insert new SI data into the control plane (also sent as TS Packets identified by their PID value).

The PID associated with an Elementary Stream can be modified (e.g. in some systems by reception of an updated SI table, or in other systems until the next announcement/discovery data is received). An attacker that is able to modify the content of the received multiplex (e.g. replay data and/or control information) could inject data locally into the received stream with an arbitrary PID value.

One method to provide security is to secure the entire Stream at the MPEG-2 TS level. This stream of TS Packets carried in a multiplex are usually received by many Receivers. The approach is well-suited to TV-transmission, data-push, etc, where the PID carries one or a set of flows (e.g. video/audio Packetized Elementary Stream (PES) Packets) with similar security requirements.

Where a ULE Stream carries a set of IP traffic flows to different destinations with a range of properties (multicast, unicast, etc), it is often not appropriate to provide IP confidentiality services for the entire ULE Stream. For many expected applications of ULE, a finer-grain control is therefore required, at least permitting control of data confidentiality/authorisation at the level of a single MAC/NPA address. However there is only one valid source of data for each MPEG-2 Elementary Stream, bound to a PID value. This observation could simplify the requirement for authentication of the source of a ULE Stream.

3.2. Threats

The simplest type of network threat is a passive threat. It includes 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 threats. An example of such a threat is an intruder monitoring the MPEG-2 transmission broadcast and then extracting traffic information concerning the communication between IP hosts using a link. Another example is of an intruder trying to gain information about the communication parties by monitoring their ULE Receiver NPA addresses;

an intruder can gain information by determining the layer 2 identity of the communicating parties and the volume of their traffic. This is a well-known issue in the security field; however it is more problematic in the case of broadcast networks such as MPEG-2 transmission networks.

Active threats (or attacks) are, in general, more difficult to implement successfully than passive threats, and usually require more sophisticated resources and may require access to the transmitter. Within the context of MPEG-2 transmission networks, examples of active attacks are:

- Masquerading: 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.
- Replay attacks: When an intruder sends some old (authentic) messages to the Receiver. In the case of a broadcast link, access to previous broadcast data is easy.
- 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.

The active threats mentioned above are major security concerns for the Internet community. The defence against such attacks is data integrity using cryptographic techniques and sequence numbers [BELLOVIN].

3.3. Threat Scenarios

Analysing the topological scenarios for MPEG-2 Transmission Networks in section 1, the security threat cases can be abstracted into three cases:

- 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). In this scenario, measures must be taken to protect the ULE data and the identity of ULE Receivers.

- 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). The MPEG transmission network operator might not be aware of such attacks. Measures must be taken to ensure ULE source authentication and preventing replay of old messages.

- 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. The requirements here are similar to scenario 2. The MPEG transmission network operator can usually identify such attacks and may resort to some means to restore the original transmission.

In terms of priority, case 1 is considered the major threat in MPEG transmission systems. Case 2 is likely to a lesser degree within certain network configurations. Hence, protection against such active actives should be used only when such a threat is a real possibility. Case 3 is envisaged to be less practical, because it will be very difficult to pass unnoticed by the MPEG transmission operator. It will require restoration of the original transmission. Therefore case 3 is not considered further in this document.

4. Security Requirements for IP over MPEG-2 TS

From the threat analysis in section 3, the following security requirements can be derived:

- Data confidentiality is the major requirement to mitigate passive threats in MPEG-2 broadcast networks.

- Protection of Layer 2 NPA address. In broadcast networks this can be used to prevent an intruder tracking the identity of ULE Receivers and the volume of their traffic.

- ULE source authentication is required against active attacks described in section 3.2.

- Protection against replay attacks. This is required for the active attacks described in section 3.2.

- Layer L2 ULE Receiver authorisation: This is normally performed during the initial key exchange and authorisation phase, before the ULE Receiver can join a secure session with the ULE Encapsulator (ULE source).

Other general requirements are:

- Decoupling of ULE key management functions from ULE security services such as encryption and source authentication. This allows the independent development of both systems.

- Traceability: To monitor transmission network using log files to record the activities in the network and detect any intrusion.

- Integrity of control and management messages in MPEG-2 transmission networks such as the SI tables (see Figure 1).

- Compatibility with other networking functions such as NAT Network Address Translation (NAT) [RFC3715] or TCP acceleration can be used in a wireless broadcast networks.

Examining the threat cases in section 3.3, the security requirements for each case can be summarised as:

- 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 source authentication using Message Authentication Code or TESLA [RFC4082] and using sequence numbers to prevent replay attacks. This will significantly reduce the ability of intruders to inject their own data into the MPEG-TS stream.

  However, scenario 2 threats apply only in specific service cases and therefore source authentication and protection against replay attacks are OPTIONAL. Such measures incur extra link transmission and processing overheads.

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

5. IPsec and MPEG-2 Transmission Networks

The security architecture for the Internet Protocol [RFC4301] describes security services for traffic at the IP layer. This architecture primarily defines services for Internet Protocol (IP) unicast packets, as well as manually configured IP multicast packets. It is possible to use IPsec to secure ULE links. The major advantage

of IPsec is its wide implementation in IP routers and hosts. IPsec in transport mode can be used for end-to-end security transparently over MPEG-2 transmission links with little impact.

In the context of MPEG-2 transmission links, if IPsec is used to secure a ULE link, then the ULE Encapsulator and Receivers are equivalent to the security gateways in IPsec terminology. A security gateway implementation of IPsec uses tunnel mode. Such usage has the following disadvantages:

- o There is an extra overheads associated with using IPsec in tunnel mode, i.e. the extra IP header (IPv4 or IPv6).

- o There is a need to protect the identity (NPA) of ULE Receivers over the ULE broadcast medium; IPsec is not suitable for providing this service. In addition, the interfaces of these devices do not necessarily have IP addresses (they can be L2 devices).

- o Multicast is considered a major service over ULE links. The current IPsec specifications [RFC4301] only define a pairwise tunnel between two IPsec devices with manual keying. Work is in progress in defining the extra detail needed for multicast and to use the tunnel mode with address preservation to allow efficient multicasting. For further details refer to [WEIS06].

6. Motivation for ULE link-layer security

Examination of the threat analysis and security requirements in sections 3 and 4 has shown that there is a need to provide link-layer (L2) security in MPEG-2 transmission networks employing ULE.

ULE link security (between a ULE Encapsulation Gateway to Receivers) is therefore considered an additional security mechanism to IPsec, TLS, and application layer security, not a replacement. It allows a network operator to provide similar functions to that of IPsec [RFC4301], but in addition provides MPEG-2 transmission link confidentiality and protection of ULE Receiver identity (NPA).

A modular design to ULE Security may allow it to use and benefit from IETF key management protocols, such as the Multicast Security group (MSEC) GSAKMP [RFC4535] and GDOI [RFC3547] protocols. This does not preclude the use of other key management methods in scenarios where this is more appropriate.

6.1. Link security below the Encapsulation layer

Link layer security can be provided at the MPEG-TS level (below ULE).

MPEG-TS encryption encrypts all TS Packets sent with a specific PID value. However, MPEG-TS may typically multiplex several IP flows, belonging to different users, using a common PID. Therefore all multiplexed traffic will share the same security keys.

This has the following advantages:

- The bit stream sent on the broadcast network does not expose any L2 or L3 headers, specifically all addresses, type fields, and length fields are encrypted prior to transmission.

- This method does not preclude the use of IPsec, or any other form of higher-layer security.

However it has the following disadvantages:

- Each ULE Receiver needs to decrypt all MPEG-2 TS Packets with a matching PID, possibly including those that are not required to be forwarded. Therefore it does not have the flexibility to separately secure individual IP flows.

- ULE Receivers will have access to private traffic destined to other ULE Receivers, since they share a common PID and key.

- Encryption of the MPE MAC address is not permitted in such systems.

- IETF-based key management are not used in existing systems. Existing access control mechanisms have limited flexibility in terms of controlling the use of key and rekeying. Therefore if the key is compromised, then this will impact several ULE Receivers.

In practice there are few L2 security systems for MPEG transmission networks. Conditional access for digital TV broadcasting is one example. However, this approach is optimised for TV services and is not well-suited to IP packet transmission. Some other systems are specified in standards such MPE [ETSI-DAT], but there are currently no known implementations.

6.2. Link security as a part of the Encapsulation layer

Examining the threat analysis in section 3 has shown that protection of ULE link from eavesdropping and ULE Receiver identity are major requirements. In the context of active threats in MPEG-2 transmission networks, ULE source authentication is required by the ULE Receivers. Attacks such as masquerading, modification of messages and injecting IP packets are more difficult, but possible as presented in threat

cases 2 and 3 (see section 3).

There are several major advantages in using ULE link level security:

- The protection of the complete ULE Protocol Data Unit (PDU) including IP addresses. The protection can be applied either per IP flow or per Receiver NPA address.

- Ability to protect the identity of the Receiver within the MPEG-2 transmission network.

- Efficient protection of IP multicast over ULE links.

- Transparency to the use of Network Address Translation (NATs) [RFC3715] and TCP Performance Enhancing Proxies (PEP) [RFC3135], which require the ability to inspect and modify the packets sent over the ULE link.

This method does not preclude the use of IPsec at L3 (or TLS [RFC4346] at L4). IPsec also provides a proven security architecture defining key exchange mechanisms and the ability to use a range of cryptographic algorithms. ULE security can make use of these mechanisms and algorithms.

7. Summary

This document 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. This includes a need to provide L2 encryption and ULE Receiver identity protection.

There is an addition need (optional) for L2 source authentication and protection against insertion of other data into the ULE stream (i.e. data integrity). This is optional because of the associated overheads for the extra features and they are only required for specific service cases.

8. Security Considerations

Link-level (L2) encryption of IP traffic is commonly used in broadcast/radio links to supplement End-to-End security (e.g. provided by TLS [RFC4346], SSH [RFC4251], IPsec [RFC4301). A common objective is to provide the same level of privacy as wired links. An ISP or User may also wish to provide end-to-end security services to the end-users (based on well known mechanisms such as IPsec or TLS).

This document provides a threat analysis and derives the security requirements to provide optional link encryption and link-level integrity / authentication of the SNDU payload.

9. IANA Considerations

This document does not define any protocol and does not require any IANA assignments.

10. Acknowledgments

The authors acknowledge the help and advice from Gorry Fairhurst (University of Aberdeen). The authors also acknowledge the contributions from Stephane Coombes (ESA) and Prof. Yim Fun Hu (University of Bradford).

11. References

11.1. Normative References

[ISO-MPEG2] "Information technology -- generic coding of moving pictures and associated audio information systems, Part I", ISO 13818-1, International Standards Organisation (ISO), 2000.

[RFC2119] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 1997.

11.2. Informative References

[ID-AR] G. Fairhurst, M-J Montpetit "Address Resolution Mechanisms for IP Datagrams over MPEG-2 Networks", Work in Progress <draft-ietf-ipdvb-ar-xx.txt.

[IEEE-802.2]"Local and metropolitan area networks-Specific requirements Part 2: Logical Link Control", IEEE 802.2, IEEE Computer Society, (also ISO/IEC 8802-2), 1998.

[ISO-8802-2]ISO/IEC 8802.2, "Logical Link Control", International Standards Organisation (ISO), 1998.

[ITU-H222] H.222.0, "Information technology, Generic coding of moving pictures and associated audio information Systems", International Telecommunication Union, (ITU-T), 1995.

[RFC4259] Montpetit, M.-J., Fairhurst, G., Clausen, H., Collini-

Nocker, B., and H. Linder, "A Framework for Transmission of IP Datagrams over MPEG-2 Networks", IETF RFC 4259, November 2005.

[RFC4326] Fairhurst, G. and B. Collini-Nocker, "Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)", IETF RFC 4326, December 2005.

[ETSI-DAT] EN 301 192, "Digital Video Broadcasting (DVB); DVB Specifications for Data Broadcasting", European Telecommunications Standards Institute (ETSI).

[BELLOVIN] S., "Problem Area for the IP Security protocols", Computer Communications Review 2:19, pp. 32-48, April 989. http://www.cs.columbia.edu/~smb/

[RFC4082] A. Perrig, D. Song, " Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", IETF RFC 4082, June 2005.

[RFC4535] H Harney, et al, "GSAKMP: Group Secure Association Group Management Protocol", IETF RFc 4535, June 2006.

[RFC3547] M. Baugher, et al, "GDOI: The Group Domain of Interpretation", IETF RFC 3547.

[WEIS06] Weis B., et al, "Multicast Extensions to the Security Architecture for the Internet", <draft-ietf-msec-ipsec-extensions-02.txt>, June 2006, IETF Work in Progress.

[RFC3715] B. Aboba and W Dixson, "IPsec-Network Address Translation (NAT) Compatibility Requirements" IETF RFC 3715, March 2004.

[RFC4346] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", IETF RFC 4346, April 2006.

[RFC3135] J. Border, M. Kojo, eyt. al., "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations", IETF RFC 3135, June 2001.

[RFC4301] Kent, S. and Seo K., "Security Architecture for the Internet Protocol", IETF RFC 4301, December 2006.

[RFC3819] Karn, P., Bormann, C., Fairhurst, G., Grossman, D.,

Ludwig, R., Mahdavi, J., Montenegro, G., Touch, J., and L. Wood, "Advice for Internet Subnetwork Designers", BCP 89, IETF RFC 3819, July 2004.

[RFC4251] T. Ylonen, C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", IETF RFC 4251, January 2006.

Author's Addresses

Haitham Cruickshank
Centre for Communications System Research (CCSR)
University of Surrey
Guildford, Surrey, GU2 7XH
UK
Email: h.cruickshank@surrey.ac.uk

Sunil Iyengar
Centre for Communications System Research (CCSR)
University of Surrey
Guildford, Surrey, GU2 7XH
UK
Email: S.Iyengar@surrey.ac.uk

Laurence Duquerroy
Research Department/Advanced Telecom Satellite Systems
Alcatel Space, Toulouse
France
E-Mail: Laurence.Duquerroy@space.alcatel.fr

Prashant Pillai
Mobile and Satellite Communications Research Centre
School of Engineering, Design and Technology
University of Bradford
Richmond Road, Bradford BD7 1DP
UK
Email: P.Pillai@bradford.ac.uk

Intellectual Property Statement

made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement