Internet Engineering Task Force
Internet Draft
draft-cruickshank-ipdvb-sec-05.txt
Expires: January 13, 2009

H. Cruickshank
University of Surrey, UK
P. Pillai
University of Bradford, UK
S. Iyengar
Logica, UK

Category: Internet draft
July 14, 2008

Security Extension for Unidirectional Lightweight Encapsulation Protocol

draft-cruickshank-ipdvb-sec-05.txt

Status of this Draft

This Internet-Draft will expire on January 13, 2009.

Abstract

This document describes the header extension for Unidirectional Encapsulation Protocol (ULE) that secures the IP traffic transported using ULE to provide security features like data confidentiality, data integrity, data origin authentication and mechanisms to prevent replay attacks. The format of the header extension and processing at the Receiver and Transmitter are

described in detail.

Table of Contents

1. Introduction

The Unidirectional Lightweight Encapsulation Protocol (ULE) [3] is used for the transportation of user traffic like IP datagrams, ethernet frames, etc. over ISO MPEG-2 Transport Streams (TS) [1]. This document describes a new ULE mandatory extension header for providing link layer security for ULE.

In MPEG-2 transmission networks employing ULE, there is a need to provide link-layer security, particularly where network layer and transport-layer security may not be present or may not be sufficient. The security requirements are presented and discussed in detail in [4]. The set of security services that the security extension for ULE can provide includes data confidentiality, data integrity, data origin authentication and rejection of replayed packets. While providing suitable link encryption is mandatory, link layer data integrity and data origin authentication is provided as an optional security service. These are especially desirable for systems where there are several ULE transmitters

(e.g. satellite meshed systems with on-board processing).

On Securing the ULE SNDUs, security is provided at the link layer as opposed to other existing mechanisms like IP Security (IPsec) [8] that provides security at the network-layer or TLS [11] that provides transport layer security. Since these security services are provided at the link layer any network layer protocol like IP (even with Ethernet bridging) may be used with secure ULE.

ULE may use and benefit from IETF key management protocols, such as the MSEC Group Domain of Interpretation (GDOI) [9] and Group Secure Association Key Management Protocol (GSAKMP) [7]. This does not preclude the use of other key management methods in scenarios for which there is benefit. The encryption algorithms, key lengths, etc. will be defined making use of the standard IPsec suites. For this purpose a security association identity similar to the IPsec Security Parameter Index (SPI)[8] is used.

In some current encapsulation methods like Multi-Protocol Encapsulation (MPE) [5], encryption of the MAC address requires each receiver to decrypt all encrypted data sent using a TS Logical Channel (identified by a PID), before it can then filter the PDUs that matches the set of Network Point of Attachment (NPA) addresses that the Receiver wishes to receive. Therefore encryption of the MPE NPA address is not permitted in such systems. This document specifies a method which provides support for using temporary Layer 2 NPA address.

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 [2].

3. Abbreviations used in the document

AES - Advanced Encryption Standard

DVB - Digital Video Broadcasting

GDOI - Group Domain of Interpretation

GSKAMP - Group Secure Association Key Management Protocol

IPsec - Internet Protocol Security

MPE - Multi-Protocol Encapsulation

MAC - Message Authentication Code

NAT - Network Address Translation

NCC - Network Control Centre

NPA - Network Point of Attachment

PEP - Protocol Enhancing Proxy

PID - Packet Identifier

PDU - Protocol Data Unit

SAD - Security Association Database

SHA - Standard Hash Algorithm

SNDU - Subnetwork Data Unit

SPD - Security Policy Database

SPI - Security Parameter Index

TLS - Transport Layer Security

ULE - Unidirectional Lightweight Encapsulation Protocol

4. ULE Security Extension

This section describes the security services offered and the packet format of the security extension for ULE. The procedures for processing the security extension header at the transmitter and the receiver are also described.

4.1. Security Services

MPEG-2 based networks are susceptible to several security attacks, both passive and active. Some of the main security services (mandatory or optional) that the security extension for ULE aims to provide for IP services running on MPEG-2 based systems are:

o Data Confidentiality (Mandatory): Data confidentiality is achieved by encrypting the higher layer PDU (and other ULE

extensions headers that may be present and require security) before encapsulation in the ULE SNDU, so that only authorised receivers can decrypt the transmitted information while an adversary would not be able to recover the important information even if it got hold of the transmitted data.

- Receiver NPA address hiding (optional): The SNDU type that is visible to all receivers has the value "encrypted content", whereas the type of PDU being carried is described using a field within the encrypted payload. This is an important objective for ULE security to prevent any passive attacks like traffic analysis. The option D=1 (i.e. no NPA address present) is permitted as long as the ULE_Security_Identifier (ULE-SID) is unique in the whole ULE network. This implies the need for a centralised key management system that generates the ULE-SID. If an NPA address is used (option D=0) in the base ULE header and NPA address hiding is utilized, then encrypted NPA address should be used. The combination of the ULE-SID and encrypted NPA will guarantee the uniqueness of the security association even in the case of a decentralized key management system.

- Data origin authentication (Optional): Data origin (source) authentication allows a ULE receiver to verify that the data is sent by the claimed ULE sender. To achieve data origin authentication, a Message Authentication Code (MAC) is generated for each message using a shared secret key and is also transmitted along with the data. The ULE receiver calculates the MAC for the received data using the shared key, and then compares this computed MAC value to the one sent by the sender along with the data. If the two match, then the receiver knows that the data had to be sent from the claimed sender.

- Data Integrity (Optional): Data integrity provides a way for the receiver of the data message to know if the data has been tampered in transit by an attacker. The MAC used for data authentication also provides data integrity. The receiver of the data calculates the MAC and compares it to the one transmitted by the sender. If an adversary had tampered with the message then the two MACs would not match.

- Replay Attacks Countermeasures (Optional): Methods against replay attacks need to ensure that the received data is recent and that an adversary has not replayed old messages at a later

time. A monotonically increasing sequence number would be used with every message and messages with old sequence number values would be rejected. The choice of using sequence numbers is dictated by policy and is done by the key management system.

Another issue is key space. There is a need for the following two databases for the correct processing on security in ULE transmitters and receivers:

- Security Policy Database (SPD): This database contains the policies that determine the processing of all ULE inbound/outbound traffic (such as encrypting all outbound ULE traffic destined to a certain terminal).

- Security Association Database (SAD): Each entry defines the parameters associated with one ULE-SID such as encryption keys, keys and algorithms used for calculating the MAC, presence of Sequence number and MAC. Each ULE-SID has an entry in the SAD.

This specification may re-use existing techniques in IPsec architecture and therefore the SPD and the SAD will follow the format of these databases as defined in RFC 4301 [8]. The security suite of algorithms for data encryption and data authenticity/integrity specified in IPsec/MSEC will be used for ULE security. The design of these databases will be simpler and also the lookups because unlike in IPsec only the ULE-SID along with the NPA address and possibly the PID is needed to retrieve the data from these databases.

4.2. Secure ULE SNDU Format

The security extension aims to secure the transmission of user traffic over MPEG-2 Transport Streams. In order to address the security issues, Figure 1 shows the SNDU format with the security extension header.

This security extension is a standard extension header as described in Section 5 of RFC 4326 [3] and does not affect the ULE base protocol. This security extension header is a Mandatory ULE Extension header. This means that a receiver MUST process this header before it processes the next extension header or the encapsulated PDU, otherwise the entire SNDU should be discarded.

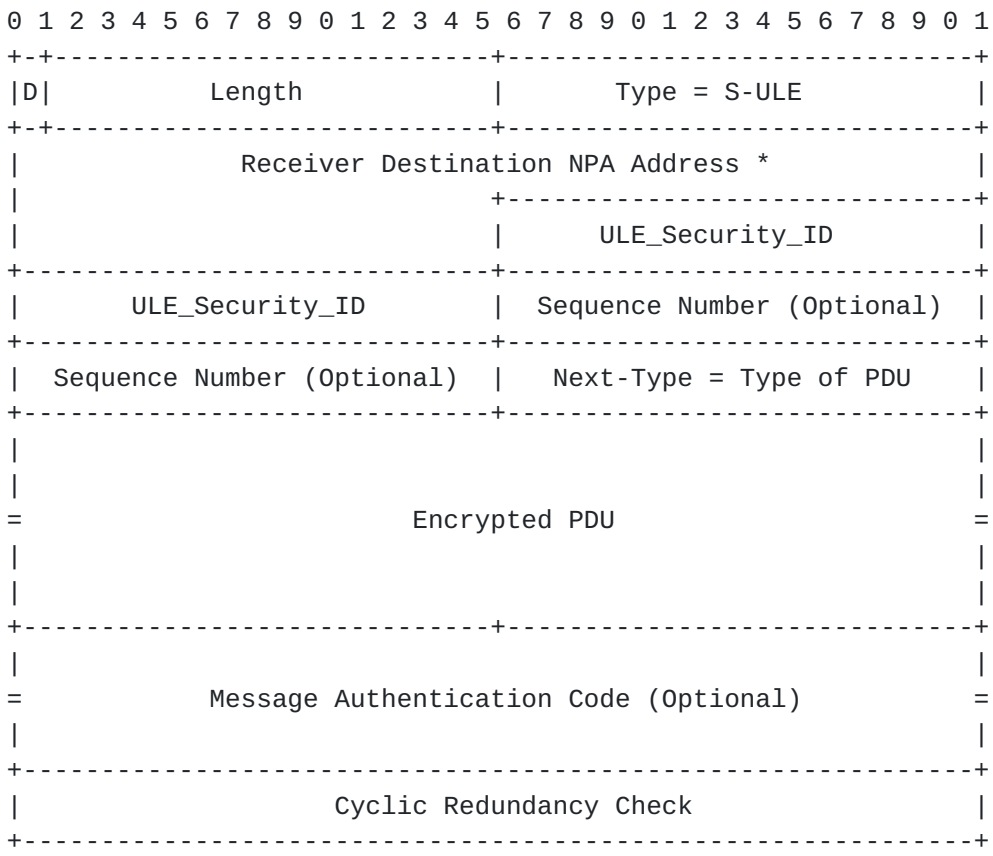


Figure 1 General SNDU format with Security extension header (D=0)

In Figure 1, the Type field in the base header denotes that a mandatory security extension header is present. The receiver destination NPA address is optional. After the base ULE header the security extension header follows. This header contains the ULE-SID, the optional Sequence Number field and the optional Message Authentication Code (MAC) field. The Next-Type field denotes the type of the enclosed PDU. The higher-layer PDU is encrypted and then encapsulated in the SNDU.

The format of the Destination Address Absent field (D), the Length field the Type field and the Receiver Destination NPA address field are defined by ULE [3].

4.2.1. Destination Address Absent (D) Field

The most significant bit of the Length Field carries the value of the Destination Address Absent Field (D) as defined by ULE [3].

When D is set to 0, it indicates the presence of the Destination Address Field while D set to 1 indicates that a Destination Address Field is not present.

4.2.2. Length Field

A 15-bit Length field denotes the length, in bytes, of the SNDU counted from the byte following the Type field, up to and including the CRC [3].

4.2.3. Type Field

A 16-bit Type Field indicates that this is a Secure ULE SNDU [3].

[XXX IANA ACTION REQUIRED to allocate xxS-ULExx XXX]

The S-ULE header is defined in the IANA maintained Next-Header Registry for ULE and has the value xxS-ULExx

[XXX END of IANA ACTION XXX]

4.2.4. Destination NPA Address Field

The SNDU Destination Address Field is optional. This field is MUST be carried when field D is set to 0 and may be omitted when D=1 [3].

4.2.5. ULE-SID Field

A 32-bit security identifier, the ULE-SID similar to the SPI used in IPsec has been added to uniquely identify the secure session. This ULE-SID represents the security association between the MPEG-2 transmitter and receiver for a particular session and indicates the keys and algorithms used for encrypting the data payload and calculating the MAC. The ULE-SID is used by a receiver to filter PDUs in combination with the NPA address when present.

4.2.6. Sequence Number Field

An optional 32-bit sequence number MAY be included in the ULE SNDU to prevent replay attacks. The gateway monotonically increments this number when it sends a packet to the receiver and the receiver verifies the correct sequence number and MUST discard all SNDUs which do not match. If an adversary tries to inject or replay old packets the sequence number would not match. This would result in discarding the packet.

SNDU reordering is not permitted on ULE links, and therefore any accidental reordering of segments will result in discard.

4.2.7. Type Field

This second type field denotes the type of packet that is encrypted and encapsulated in the Secure ULE SNDU. If another ULE extension header follows, then this type field indicates the type of this extension header.

4.2.8. Encrypted SNDU Payload

To achieve data confidentiality, the traffic between the MPEG-2 TS transmitter (ULE Encapsulator) and Receiver needs to be encrypted. The network layer PDUs are first encrypted and then encapsulated in the secure ULE SNDU. The security associations between the two communicating points will describe the algorithms and keys used for encryption purposes.

Secure ULE does not impose the use of any specific encryption algorithm and should be able to support the commonly used algorithms including DES [12], 3DES etc.

4.2.9. Message Authentication Code (MAC) Field

To provide both data origin authentication and data integrity, a Message Authentication Code (MAC) is included in the extension header.

The MAC is calculated over the ULE security extension header and the encrypted data payload. The receiver calculates the MAC for the each received packet and compares it with the transmitted value. The two would not match in only 2 cases, firstly either there was an error during processing or transmission over the MPEG-2 Network, or secondly the packet has not been sent from an authenticated entity. In either case, the packet MUST be discarded. Hence the same MAC can be used for data origin authentication and to provide data integrity for transmission/processing errors.

4.3. Transmitter Processing

The following procedure is followed at the encapsulator for processing the security extension header for ULE:

- Upon reception of the higher layer PDU, the SPD is first queried to check the policy to be applied to the PDU. If

security is needed then an SA must exist in the SAD (this is set by the key management system). The parameters are retrieved from the SAD and it is first encrypted using the key and the algorithm as indicated in the SAD.

- The header of the base protocol (and other extension headers if present) is added to the SNDU.

- The ULE-SID for the security association between the transmitter and the receiver are added next.

- The SAD is consulted to determine if the sequence number has to be added. If required, then the corresponding sequence number is added to the SNDU.

- Then the encrypted higher layer PDU is encapsulated to form the SNDU.

- The SAD is then checked to determine if the data origin authentication and data integrity has to be provided. If required, then the MAC has to be calculated. The MAC is calculated over the encrypted PDU (and other possible extension headers), the Security extension header and the secret key. The MAC is then added to the extension header in the SNDU.

- Finally, the CRC is calculated as defined in Section 4.6 of RFC4326 [3] and added.

4.4. Receiver Processing

The following procedure is followed at the Receiver for processing the security extension header for ULE:

- Upon reception of a Secure ULE SNDU, the Receiver first filters the received packets according to the receiver destination NPA address (if present).

- The CRC is verified as defined in RFC4326 [3].

- The Receiver then uses the ULE-SID to obtain the security associations between the transmitter and receiver and retrieve the data from the SAD. With this the receiver determines if the sequence number and the MAC are present or not. This is also used to determine the algorithms and keys used for both encryption of the encapsulated PDU and for generation of the message authentication code.

- o If present the next step would be to check the MAC to verify the authenticity and integrity of the received PDU. If the calculated MAC does not match the transmitted MAC, then the PDU is discarded.

- o It would then use the sequence number for filtering any out of-sequence packets.

- o Finally the encapsulated payload will be decrypted.

5. Key Exchange Procedure

This section describes the key exchange procedure, used to install and manage the keys at Receivers. There is a need to take into account the two cases described in [10], both unidirectional and bi-directional transfers. The key management procedures are independent from the ULE operations. During the key exchange procedure, the ULE-SID will be defined.

The exact data encryption and data integrity choices are linked to the key management systems in use. One example is the security suite 1 (defined in GSAKMP [7]). This uses AES (CBC mode, Key Length: 128 bits) for data encryption and DSS-ASN1-DER for digital signature and SHA-1 as the Hash algorithm. Other suites will be added in future versions.

A detailed key management system is not presented in this document, but two approaches are outlined.

5.1. IPsec Key Management for L2

Existing key management systems can be used such as the MSEC key exchange protocols, GDOI and GSAKMP. The format of the ULE-SID will be identical to the security association as defined in GDOI or GSAKMP. The initial key exchange between the security server and the ULE receiver can be transported either within the ULE network or may be performed by some other means. This is a matter of policy and an architecture decision. For example, for bi-directional transfers the whole key exchange procedures could be carried within the ULE network, while for unidirectional transfers, some other bidirectional connection should be used.

5.2. Alternative Key Management

The method described here for link security may be used with alternative key management systems when used as a part of a system that already implements a key management infrastructure

(e.g. the DVB-RCS security system [6]). The format of the ULE-Security-ID will be the same format as defined in DVB-RCS security procedures.

6. Secure ULE SNDU example

This section shows the ULE SNDU with the security extension header when IP datagrams are secured using Secure ULE. In the example below, there are no additional extension headers.

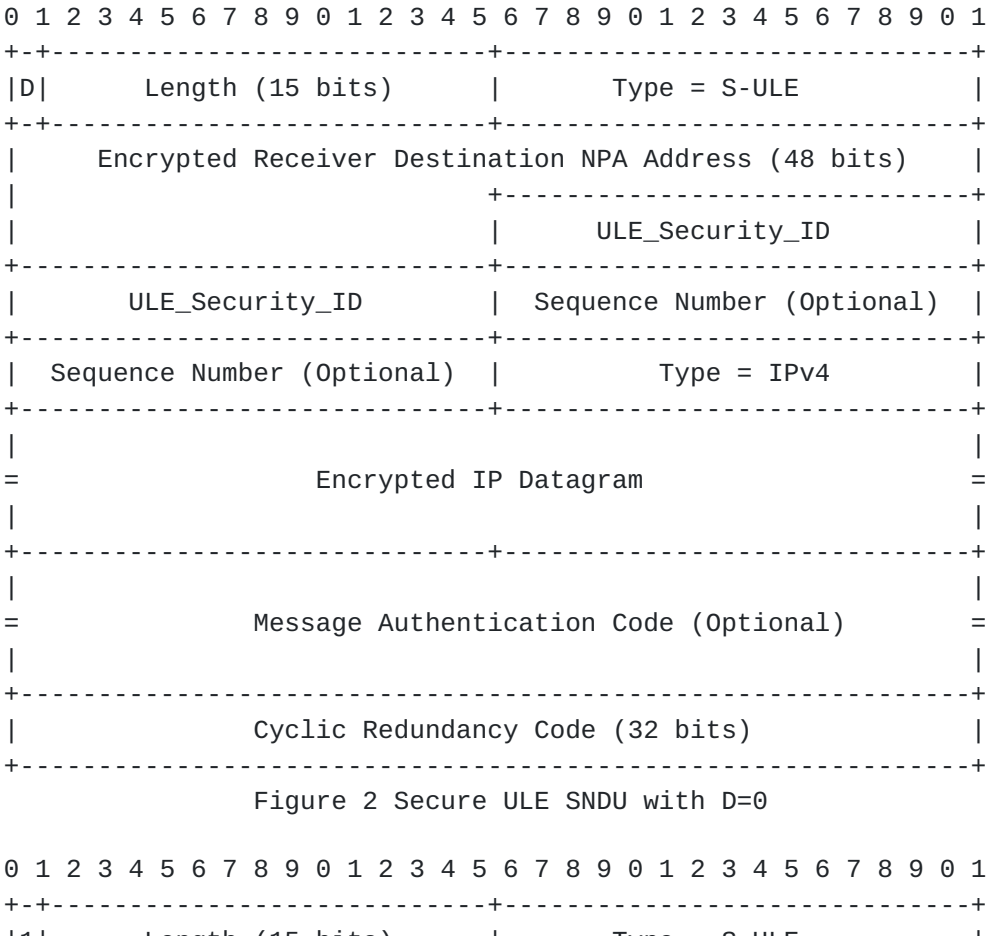
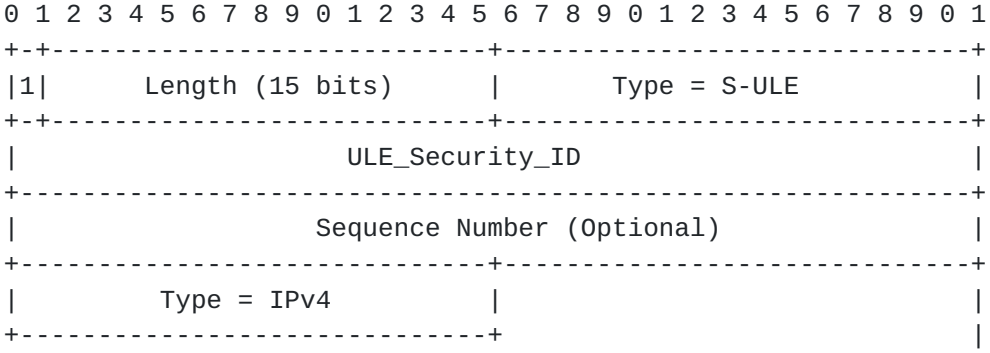


Figure 2 Secure ULE SNDU with D=0



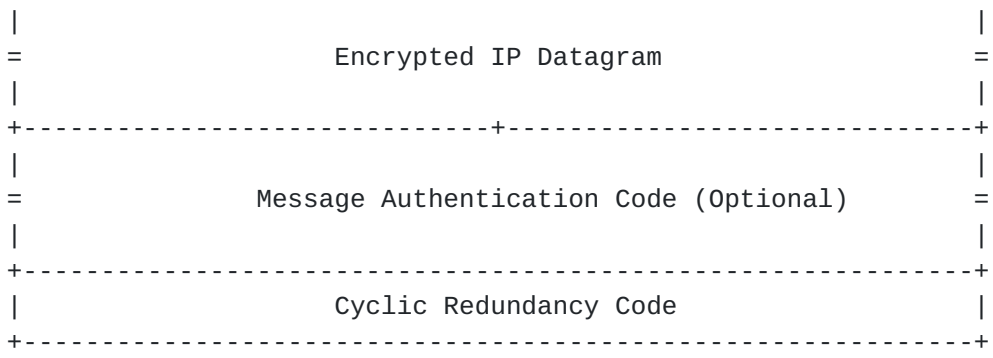


Figure 3 Secure ULE SNDU with D=1

7. 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, SSH, Open PGP, S/MIME, IPsec). A common objective is to provide the same level of privacy as terrestrial links. This document defines a method to provide mandatory link encryption at the ULE level. The method may also support optional link level integrity / authentication of the SNDU payload plus protection against replay attacks. This is provided in a flexible way using a new ULE Mandatory Extension Header for security. This decouples specification of the security functions from the encapsulation functions. This method also supports encryption of the NPA addresses. The encryption and integrity algorithms are similar to the ones used in IPsec/MSEC protocols.

8. IANA Considerations

The S-ULE header is defined in the IANA maintained Next-Header Registry for ULE and has the value xxS-ULExx

9. Acknowledgments

The authors acknowledge the help and advice from Gorry Fairhurst (University of Aberdeen), L. Duquerroy (Alcatel Alenia Space) Stephane Coombes (ESA) and Yim Fun Hu (University of Bradford) in the preparation of this document.

10. References

10.1. Normative References

[1] ISO/IEC DIS 13818-1, "Information technology - Generic codeing of moving pictures and associated audio information

- Part1: Systems", International Standards Organisation (ISO)

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[4] H. Cruickshank, S. Iyengar and P. Pillai, "Security requirements for the Unidirectional Lightweight Encapsulation (ULE) protocol", draft-ietf-ipdvb-sec-req-07.txt, June 17, 2008.

10.2. Informative References

[5] "Digital Video Broadcasting (DVB): DVB Specifications for Data Broadcasting", ETSI EN 301 192 v1.3.1, 2003.

[6] "Digital Video Broadcasting (DVB): Interaction Channel for satellite distribution systems", ETSI EN 301 790 v1.4.1, 2005.

[7] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, June 2006.

[8] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[9] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[10] Montpetit, M., Fairhurst, G., Clausen, H., Collini-Nocker, B., and H. Linder, "A Framework for Transmission of IP Datagrams over MPEG-2 Networks", RFC 4259, November 2005.

[11] http://www.ietf.org/html.charters/tls-charter.html

[12] National Institute of Standards and Technology, "Data encryption Standard (DES)", Federal Information Processing Standard (FIPS) Publication, FIPS PUB 46-3, October 1999.

11. 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

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

Sunil Iyengar
Space & Defence
Logica
Springfield Drive
Leatherhead
Surrey KT22 7LP
UK
Email: sunil.iyengar@logica.com

12. IPR Notices

12.1. Intellectual Property Statement

12.2. Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has 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.

13. Copyright Statement