Network Working Group
Internet-Draft
Expires: April 17, 2007

M. Baugher
Cisco Systems, Inc.
A. Rueegsegger
October 14, 2006

GDOI Key Establishment for the SRTP Data Security Protocol
draft-baugher-msec-gdoi-srtp-00.txt

Status of this Memo

Copyright Notice

Abstract

The Secure Real-time Transport Protocol (SRTP) secures unicast and multicast media streams. Multicast receivers of an SRTP stream therefore share an SRTP master key for multicast message authentication and decryption. This document describes how to establish a shared, "group key" for an SRTP session using RFC 3547, the Group Domain of Interpretation (GDOI) and RFC 2408, the Internet Security Association and Key Management Protocol. This document extends GDOI for SRTP group key establishment.

Table of Contents

1. Introduction

The Group Domain of Interpretation (GDOI) is specified in RFC 3547 [RFC3547]. GDOI is based upon ISAKMP, the Internet Security Association and Key Management Protocol [RFC2408]. GDOI extends ISAKMP for group key management whereby a cryptographic key is shared among multiple receivers. GDOI uses both unicast and multicast key establishment, and can support messaging for member revocation algorithms, such as the "key hierarchy" algorithm [RFC2627]. GDOI preserves the ISAKMP design, which supports new data security protocols through documented procedures. GDOI currently supports only one data security protocol, IPsec.

This document presents GDOI payloads for another data security protocol, the Secure Real-time Transport Protocol (SRTP). These payload definitions apply GDOI key establishment procedures to groups of SRTP receivers in accordance with Section 5.4.2 of the GDOI protocol specification [RFC3547]. GDOI carries keys, parameters, and other values needed for an SRTP session's "cryptographic context", which is described in Section 8 of the SRTP specification [RFC3711]. The GDOI-SRTP payloads MAY signal use of the EKT protocol as an option for secure dissemination of internally-generated SRTP parameters [I-D.mcgrew-srtp-ekt]. These options, parameters and keys are contained in two GDOI payloads, the "Key Download" (KD) and the "Security Association Traffic Encrypting Key" (SA-TEK) payloads.

1.1. Overview of This Document

Section 2 of this document presents the GDOI-SRTP payloads. The SRTP SA-TEK payload MAY carry IP address and port information, which has implications for network address translation (NAT). Section 3 gives NAT considerations, Section 4 discusses Security Considerations, and Section 5 lists IANA requirements.

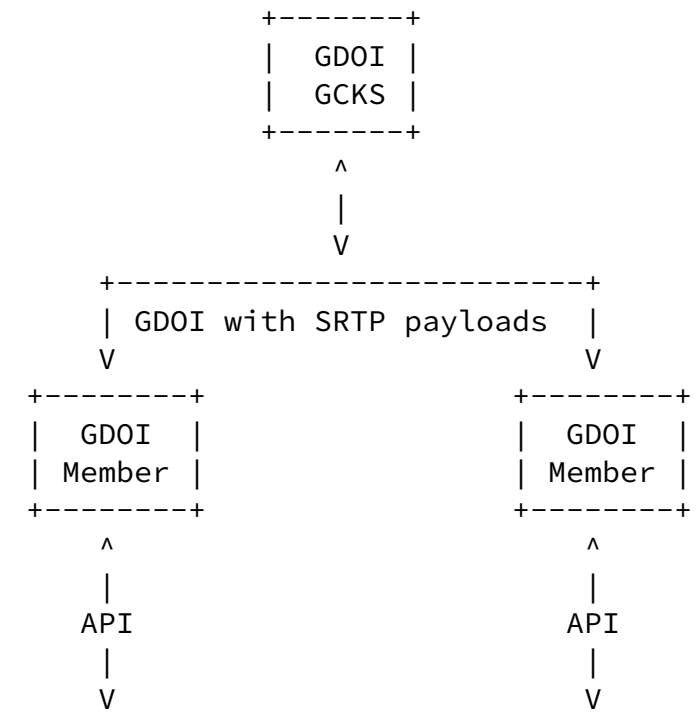
1.2. Conformance Language

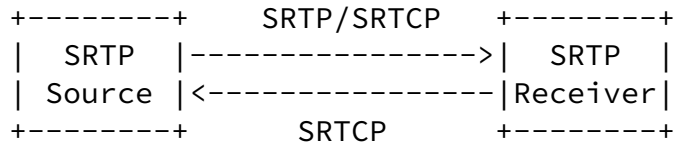
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. SRTP Definitions for GDOI Signaling

An application can use GDOI to establish security associations for a data security protocol when GDOI is extended with one or more payloads for that data security protocol. Payloads are carried in GDOI message exchanges between a GDOI Group Controller/Key Server (GCKS) and a GDOI member, as shown in Figure 2.0-1.

Figure 2.0-1: GDOI and SRTP Interfaces





This section specifies the SRTP payloads for GDOI key management exchanges. SRTP is an application-layer security protocol that operates above the TCP/IP services (sockets) interface. GDOI also operates above the transport service. SRTP communicates with GDOI using the API shown in Figure 2.0-1. Using the API, SRTP or another application requests that GDOI establish an SRTP cryptographic context (a "security association" in GDOI parlance), which is described in Section 3.2 of the SRTP specification [RFC3711]. The API of Figure 2.0-1 is not considered further in this document, which is concerned with extending the GDOI protocol with a new payload. Using this protocol extension, the GDOI Group Controller/Key Server (GCKS) provides the cryptographic keys, policies and other attributes to SRTP (via the API to a GDOI Member). The GCKS might obtain some of this information through a user console or event database, and it

generates some information automatically, such as keying materials. How the GCKS obtains or generates information for the SRTP payload fields is not considered further in this document.

Figure 2.0-2: GDOI GCKS Co-located with GDOI Member

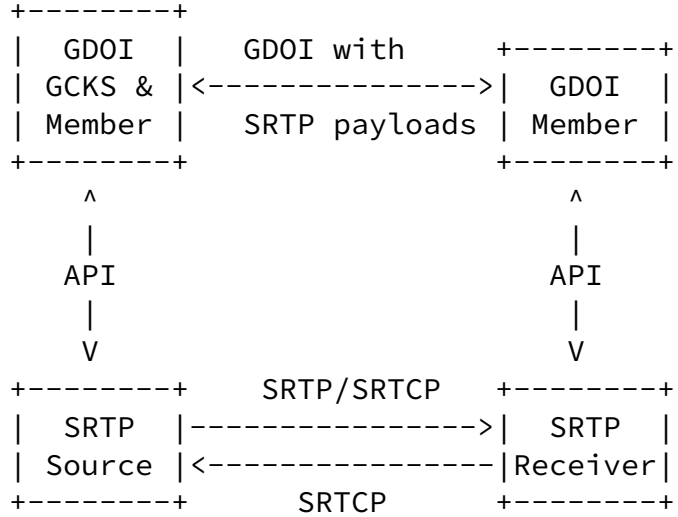


Figure 2.0-1 is a logical diagram. In a physical realization of the system, the GDOI GKCS can either be separate from or co-located with a GDOI Member. When physically co-located with a member, the GCKS can be dedicated to maintaining the group keys for that member's "SRTP Source", and the GCKS can more easily obtain the SRTP-specific information for its payloads across the API. This configuration is shown in Figure 2.0-2. It is often more efficient for the GCKS to be physically co-located in the same computer as the SRTP source of the multicast stream.

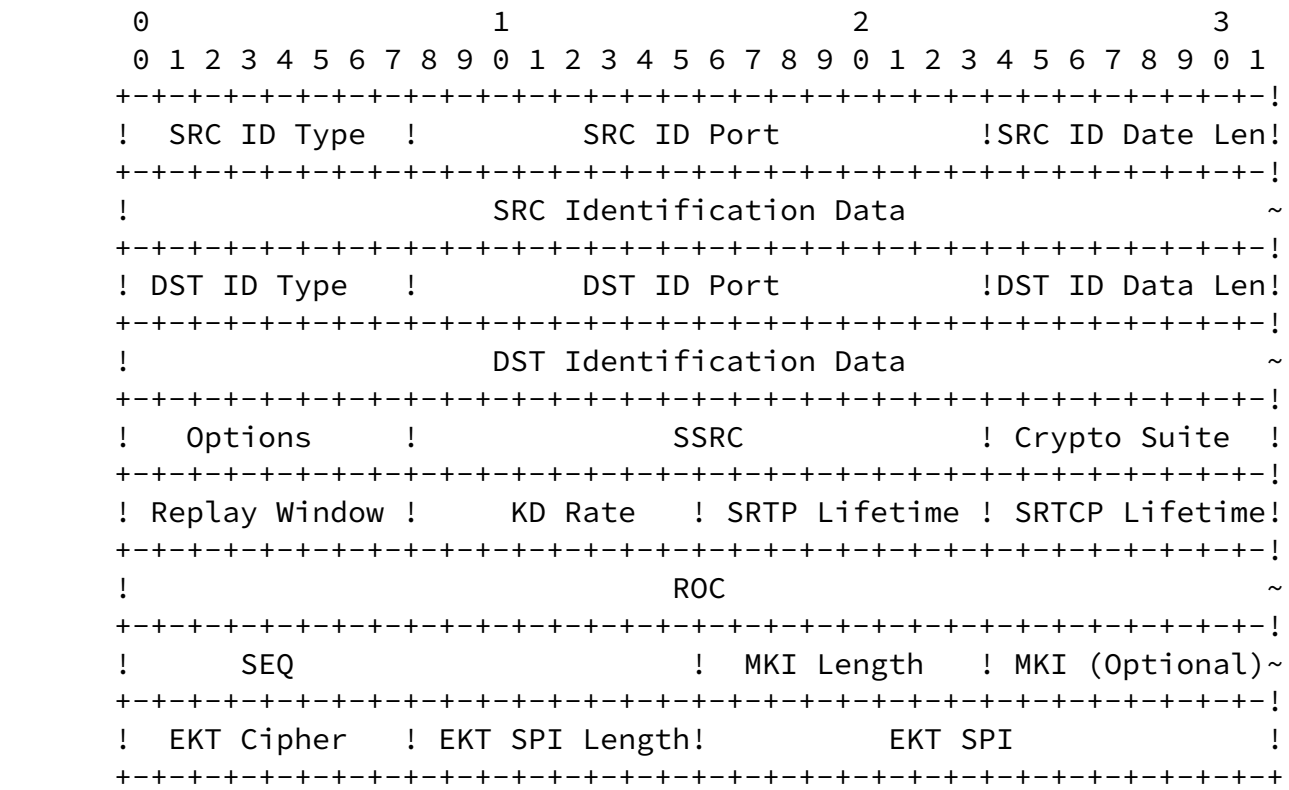
2.1. GDOI and EKT

It is not always possible for GCKS to obtain all the needed SRTP information. In order to establish an SRTP session, an SRTP system requires some internally-generated SRTP information along with keys. This information is the SSRC, the rollover counter (ROC), and the sequence number (SEQ). The ROC and SEQ are used by the SRTP ciphers, and they are used in SRTP replay protection; the SSRC is used in combination with the destination transport address to identify an RTP session [RFC3550] and thus an SRTP session's crypto context. The SEQ and ROC values are generated internally by the SRTP source. When the GCKS is co-located with the GDOI Member and the SRTP source, however, this information can be obtained via the API shown in the above figures. But when the GCKS is physically separate from the SRTP source, GDOI has no over-the-wire protocol for collecting such SSRC, ROC and SEQ information from a multicast source.

The EKT protocol offers a solution to the problem of securely providing the SSRC, ROC and the SEQ from the SRTP source to the SRTP receiver, and EKT correctly initializes the SSRC, ROC and SEQ for late joiners to the multicast or following RTP SSRC collision repair [I-D.mcgrew-srtp-ekt]. EKT is RECOMMENDED in this document for transport of an SRTP sender's SSRC, ROC and SEQ to SRTP receivers. When it is possible for the GCKS to correctly initialize the SSRC, ROC and SEQ, however, it is RECOMMENDED that the Key Download also carry the SRTP master key and salt as this will allow the SRTP receiver to begin validating and decrypting packets without waiting for an EKT message to arrive in the SRTCP. EKT is particularly useful when the GCKS cannot reliably initialize the SA-TEK with SSRC, ROC and SEQ fields. When EKT is used, the SA-TEK at minimum signals EKT in the SA-TEK Options field and provides the EKT Key in a Key Download payload.

2.2. SRTP SA-TEK Definitions

Figure 2.2-1: SRTP SA-TEK



GDOI provides SA-TEK and Key-Download payload information to an SRTP implementation, which uses this information to initialize the cryptographic context of an SRTP session. An SRTP crypto context is identified by the SSRC and RTP destination transport address as explained in Section 8 of the SRTP specification [RFC3711]. The SRTP

rollover counter (ROC) and current sequence number (SEQ) MAY be carried in the SA TEK payload that is shown in Figure 2.2-1. When the ROC and the SEQ are not carried in the SRTP SA-TEK payload, the EKT protocol SHOULD be used [I-D.mcgrew-srtp-ekt], in which case the SA-TEK carries EKT information as shown in Figure 2.2-1. In either case, GDOI-SRTP uses the same encryption and authentication transforms for SRTP and SRTCP.

The RFC 3547 SA TEK payload has a header and a protocol-specific payload. The SRTP SA TEK is identified by the GDOI_PROTO_SRTP value in the Protocol-ID field of the SA TEK header, which is defined in Section 5.4 of RFC 3547 [RFC3547]. The SA TEK protocol-specific payload for SRTP is given in Figure 2.2-1. The SAT Payload fields are defined as follows:

- SRC ID Type (1 octet) -- Value describing the identity information found in the SRC Identification Data field. Defined values are specified by the IPSEC Identification Type section in the IANA isakmpd-registry [ISAKMP-REG].

- SRC ID Port (2 octets) -- Value specifying a port associated with the SRC Identification data. A value of zero means that the SRC ID Port field should be ignored.

- SRC ID Data Len (1 octet) -- Value specifying the length of the SRC Identification Data field.

- SRC Identification Data (variable length) -- Value as indicated by the SRC ID Type. According to RFC 3547, SRC Identification Data consists of three bytes of zero for multiple-source multicast groups that use a common TEK for all senders. The TEK in an SRTP Key Download payload is an SRTP master key, however, and it is NOT RECOMMENDED that this key be shared for the counter mode and f8 ciphers of SRTP. Thus, it is NOT RECOMMENDED that this field consist of three bytes of zero. It SHOULD be ID_FQDN (see the "NAT Considerations" section).

- DST ID Type (1 octet) -- Value describing the identity information found in the DST Identification Data field. Defined values are specified by the IPSEC Identification Type section in the IANA isakmpd-registry [ISAKMP-REG].

- DST ID Port (2 octets) -- Value specifying a port associated with the source Id. A value of zero means that the DST ID Port field should be ignored.

- DST ID Data Len (1 octet) -- Value specifying the length of the DST Identification Data field.

- DST Identification Data (variable length) -- Value, as indicated

by the DST ID Type.

- Options (1 octet) - Reading from left to right (big-endian), SRTP is unencrypted when bit 0 is set to '1'. SRTP is unauthenticated when bit 1 is set to '1'. SRTCP is unencrypted when bit 2 is set to '1'. EKT is not used when bit 3 is set to '1'. The SSRC, ROC and SEQ are not included and MUST be ignored when bit 4 is set to '1'.

- SSRC (2 octets) - Value of the Sender's SSRC when there is a single sender associated with the KEK and TEK and signaled in SA-TEK and Key Download payload.

- Crypto Suite (1 octet) -- The set of parameters that defines the SRTP and SRTCP encryption transform, authentication transform, key length, and salt length. The values are defined in the Table 2.1-2. Each row in the table defines a suite of parameters. Any parameter can be changed and new parameters added by creating a new Crypto Suite, documenting it in an Internet RFC, and requesting a Suite Value for it from IANA.

  Table 2.1-2: SRTP Crypto Suites

Suite Value	Cipher	Master Keylen	Master Saltlen	Max SRTP Lifetime	Max SRTCP Lifetime	MAC/len
0	AES-CM	128	112	2^48	2^31	HMAC-SHA1/80
1	AES-CM	128	112	2^48	2^31	HMAC-SHA1/32
2	AES-F8	128	112	2^48	2^31	HMAC-SHA1/80
3	AES-CM	192	112	2^48	2^31	HMAC-SHA1/80
4	AES-CM	192	112	2^48	2^31	HMAC-SHA1/32
5	AES-CM	256	112	2^48	2^31	HMAC-SHA1/80
6	AES-CM	256	112	2^48	2^31	HMAC-SHA1/32
7-127	RESERVED					

  Note: All keylen values are in bits

  The key values of 192 and 256 are specified in the "BIG AES" Internet Draft document [I-D.mcgrew-srtp-big-aes]. In the vast majority of SRTP applications, the BIG AES values SHOULD NOT be used since they do not increase security as a practical matter but could diminish interoperability, see Section 7 of the Big AES I-D.

- Replay Window Size (1 octet) - The size of SRTP Replay Window as specified in Section 3.3.2 of the standard[RFC3711].

- KD Rate (1 octet) - SRTP Key Derivation Rate as specified in Section 4.3.1, second paragraph of the standard [RFC3711]. KD

Rate is an integer that is greater than or equal to zero. The modulus of the SRTP "packet index" of an outgoing or incoming SRTP packet is computed modulo the KD Rate in cases where the KD Rate is greater than zero. The reader is referred to Sections 3.3.1 and 4.3.1 of the SRTP specification for the definitions of "packet index" and "Key Derivation Rate".

- SRTP Lifetime (1 octet) - The SRTP key lifetime is encoded as an integer N to represent a lifetime of 2^N packets, where N cannot exceed the maximum lifetime as specified by the Crypto Suite. A value of zero signals the SRTP default.

- SRTCP Lifetime (1 octet) - The SRTCP key lifetime is encoded as an integer N to represent a lifetime of 2^N packets, where N cannot exceed the maximum lifetime as specified by the Crypto Suite. A value of zero signals the SRTP default.

- ROC (4 octets) - When bit 4 of Opions is cleared to '0', this field contains the current value of the SRTP ROC.

- SEQ (2 octets) - When bit 4 of Options is cleared to '0', this field contains the current SRTP SEQ.

- MKI Length (1 octet) - An SRTP Master Key Indicator (MKI) SHALL appear in SRTP packets when this field is nonzero. The MKI field is the length of the SRTP MKI as defined in Section 3 of RFC 3711 [RFC3711]. The maximum MKI length is 128 (bytes) though a smaller length of one or two bytes IS RECOMMENDED.

- MKI (optional, variable length) - The SRTP MKI is present when the SRTP MKI Length is nonzero. The value of the SRTP MKI Length determines the number of bytes in the width of this field.

- EKT Cipher (1 octet) - When bit 3 of the SRTP Options field is cleared to '0', EKT parameters appear in the SA TEK payload. "EKT Cipher" is the cipher and mode used by EKT for the EKT key, which is carried in a GDOI Key Download payload. The following table correlates each EKT Cipher Suite [I-D.mcgrew-srtp-ekt] with a Suite Value. New EKT Cipher Suites MAY be added when documented by an Internet RFC and once IANA assigns a Suite Value to that Cipher Suite.

Table 2.1-3: EKT Cipher Suites

EKT Cipher Suite	Suite Value
RESERVED	0
AES_128	1
AESKW_128	2
AESKW_196	3
AESKW_256	4
RESERVED	5-127

- EKT SPI Len (1 octet) - The length of the EKT SPI.

- EKT SPI (variable length) - The EKT SPI.

2.3. SRTP Key Download

The Crypto Suites of Table 2.1-2 define two keys, the SRTP master key and master salt key. These two keys are concatenated with the SRTP master key followed by the SRTP master salt in a Key Download (KD) payload's TEK_ALGORITHM_KEY attribute.

When EKT is used, EKT key is carried as a KEK_ALGORITHM_KEY attribute.

3. NAT Considerations

Transport addresses are carried in the SA-TEK payload and this contradicts recommendations for application-layer signaling through network address translators (NATs) [RFC2663][RFC3235]. The destination IP address and port, however, are multicast addresses and these are not re-written by a NAT. The source address, however, might be re-written on outgoing multicast packets [I-D.wing-behave-multicast].

If the SA TEK SRC ID type of Figure 2.1-1 is an IP address and if there is an outgoing NAT that re-writes the source IP address field of outgoing packets, then there will likely be a discrepancy between the source address in the IP packet and the SRC Identification Data field of Figure 2.1-1. It is therefore RECOMMENDED that SRC ID Type be ID_FQDN [ISAKMP-REG] whenever there is network address translation present on the network of the multicast source.

4. Security Considerations

The security of GDOI and its payloads is discussed in Section 6 of the GDOI specification [RFC3547]. The security of SRTP and its parameter settings is discussed in Section 9 of the SRTP specification[RFC3711]. There are some additional risks in GDOI and SRTP that are considered here.

4.1. No Sharing Counter-Mode Encryption Keys

One risk is to the proper establishment of the SRTP SSRC, which is subject to SSRC collisions that might be exploited by an attacker. SRTP specifies that the SSRC is used in the AES counter mode and f8 initialization vectors (IV) to prevent counter reuse. RFC 3711 states that key management "SHOULD" install a unique SSRC. GDOI relaxes this requirement since SSRCs collide. It is also difficult to support and unchanged RTP module in a "bump-in-the-stack" SRTP configuration. Instead of depending on SSRC uniqueness, IT IS RECOMMENDED that the GDOI SA-TEK SHOULD provide a unique SRTP master key for each sender.

To ensure SRTP master key uniqueness among senders to an SRTP session, SA-TEK SRC Identification Data (Figure 2.1.1) MUST NOT signal a group of senders sharing a key. GDOI specifies a means for sharing a traffic encrypting key (TEK) among senders, but a GDOI TEK

is an SRTP master key and this specification RECOMMENDS that a TEK not be shared among SRTP sources.

4.2. Enable Distributed Key Management

In many cases, SRTP sources are not co-located with a GCKS. This is one possible configuration in a large scale "video pump", for example, that is specialized to a purpose other than key management. If there are geographically-dispersed video-pump sources, there is the risk that the GCKS will be attacked and its ability to disseminate source-unique values to such as the ROC to the multicast group will be impaired. This is one possible attack out of many where a central GCKS can disrupt the entire multicast group of SRTP receivers. This document RECOMMENDS use of EKT to securely distribute the SSRC, ROC and SEQ. GDOI-SRTP payloads signal the EKT Key.

Two protocols have more vulnerabilities than one, however, and there are added risks that come from using both GDOI and EKT. A programming bug in GDOI (e.g. signaling zeros in SA-TEK SRC Identification Data), for example, might cause an attack on EKT (e.g. a distributed denial of service attack on a group of EKT receivers). In some cases, a feature that is useful for M:N groups might be risky

when used in 1:N groups. For these reasons, the GDOI-SRTP SA-TEK SHOULD explicitly signal each source and provides a source TEK (SRTP Master Key) as well as a KEK (EKT Key). In extraordinary cases such as SSRC collision, the SSRC and SRTP master key MAY come from EKT, but in normal operation only the SEQ and ROC SHOULD be obtained from EKT.

4.3. Support Strong Source Authentication

Despite the precautions described above, there is always the possibility of "source spoofing" when any member of the group authorized only to receive can impersonate an authorized sender. This is a limitation in symmetric-key authentication in secure groups. To address this problem, SRTP can use TESLA source authentication messaging [RFC4383]. A future revision of this document will consider TESLA signaling.

5. IANA Considerations

IANA is requested to register "GDOI_PROTO_SRTP with a new value and that additional values be added to the Security Association Traffic Encrypting Key payload definitions, "SA TEK Payload Values" [GDOI-REG], as follows.

1. Table 2.1-2: SRTP Crypto Suites.

2. Table 2.1-3: EKT Cipher Suites

6. Acknowledgements

The authors thank David McGrew and Brian Weis for their helpful comments.

7. References

7.1. Normative References

[GDOI-REG] "Group Domain of Interpretation (GDOI) Payloads - per [RFC3547], http://www.iana.org/assignments/gdoi-payloads", 2003.

[I-D.mcgrew-srtp-big-aes] McGrew, D., "The use of AES-192 and AES-256 in Secure RTP", draft-mcgrew-srtp-big-aes-00 (work in progress), April 2006.

[I-D.mcgrew-srtp-ekt] McGrew, D., "Encrypted Key Transport for Secure RTP", draft-mcgrew-srtp-ekt-01 (work in progress), June 2006.

[ISAKMP-REG] "FROM RFC 2407 and RFC 2408 Magic Numbers for ISAKMP Protocol, http://www.iana.org/assignments/isakmp-registry", September 2006.

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

[RFC2627] Wallner, D., Harder, E., and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, June 1999.

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC4383] Baugher, M. and E. Carrara, "The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)", RFC 4383, February 2006.

7.2. Informative References

[I-D.wing-behave-multicast]
Wing, D., "IGMP Proxy Behavior", draft-wing-behave-multicast-00 (work in progress), October 2004.

[RFC2408] Maughan, D., Schneider, M., and M. Schertler, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC3235] Senie, D., "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, January 2002.

Authors' Addresses

Mark Baugher
Cisco Systems, Inc.
800 East Tasman Drive
San Jose, CA 95164
US

Phone: (503) 245-4543
Email: mbaugher@cisco.com

Adrian-Ken Rueegsegger
Bocksteinstrasse 2
4583 Muehledorf,
Switzerland

Phone: +41 32 661 10 88
Email: adrian.rueegsegger@students.fhnw.ch

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.