Network Working Group
Request for Comments: 5124
Category: Standards Track

J. Ott
Helsinki University of Technology
E. Carrara
KTH

February 2008

Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)

Status of This Memo

Abstract

An RTP profile (SAVP) for secure real-time communications and another profile (AVPF) to provide timely feedback from the receivers to a sender are defined in RFC 3711 and RFC 4585, respectively. This memo specifies the combination of both profiles to enable secure RTP communications with feedback.

Table of Contents

1. Introduction

The Real-time Transport Protocol, the associated RTP Control Protocol (RTP/RTCP, RFC 3550) [1], and the profile for audiovisual communications with minimal control (RFC 3551) [2] define mechanisms for transmitting time-based media across an IP network. RTP provides means to preserve timing and detect packet losses, among other things, and RTP payload formats provide for proper framing of (continuous) media in a packet-based environment. RTCP enables receivers to provide feedback on reception quality and allows all members of an RTP session to learn about each other.

The RTP specification provides only rudimentary support for encrypting RTP and RTCP packets. Secure RTP (RFC 3711) [4] defines an RTP profile ("SAVP") for secure RTP media sessions, defining methods for proper RTP and RTCP packet encryption, integrity, and replay protection. The initial negotiation of SRTP and its security parameters needs to be done out-of-band, e.g., using the Session Description Protocol (SDP, RFC 4566) [6] together with extensions for conveying keying material (RFC 4567 [7], RFC 4568 [8]).

The RTP specification also provides limited support for timely feedback from receivers to senders, typically by means of reception statistics reporting in somewhat regular intervals depending on the group size, the average RTCP packet size, and the available RTCP bandwidth. The extended RTP profile for RTCP-based feedback ("AVPF") (RFC 4585, [3]) allows session participants statistically to provide immediate feedback while maintaining the average RTCP data rate for all senders. As for SAVP, the use of AVPF and its parameters needs to be negotiated out-of-band by means of SDP (RFC 4566, [6]) and the extensions defined in RFC 4585 [3].

Both SRTP and AVPF are RTP profiles and need to be negotiated. This implies that either one or the other may be used, but both profiles cannot be negotiated for the same RTP session (using one SDP session level description). However, using secure communications and timely feedback together is desirable. Therefore, this document specifies a new RTP profile ("SAVPF") that combines the features of SAVP and AVPF.

As SAVP and AVPF are largely orthogonal, the combination of both is mostly straightforward. No sophisticated algorithms need to be specified in this document. Instead, reference is made to both existing profiles and only the implications of their combination and possible deviations from rules of the existing profiles are described as is the negotiation process.

1.1. Definitions

The definitions of RFC 3550 [1], RFC 3551 [2], RFC 4585 [3], and RFC 3711 [4] apply.

The following definitions are specifically used in this document:

RTP session:
: An association among a set of participants communicating with RTP as defined in RFC 3550 [1].

(SDP) media description:
: This term refers to the specification given in a single m= line in an SDP message. An SDP media description may define only one RTP session.

Media session:
: A media session refers to a collection of SDP media descriptions that are semantically grouped to represent alternatives of the same communications means. Out of such a group, one will be negotiated or chosen for a communication relationship and the corresponding RTP session will be instantiated. If no common session parameters suitable for the involved endpoints can be found, the media session will be rejected. In the simplest case, a media session is equivalent to an SDP media description and equivalent to an RTP session.

1.2. Terminology

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 [5].

2. SAVPF Rules

SAVP is defined as an intermediate layer between RTP (following the regular RTP profile AVP) and the transport layer (usually UDP). This yields a two-layer hierarchy within the Real-time Transport Protocol. In SAVPF, the upper (AVP) layer is replaced by the extended RTP profile for feedback (AVPF).

AVPF modifies timing rules for transmitting RTCP packets and adds extra RTCP packet formats specific to feedback. These functions are independent of whether or not RTCP packets are subsequently encrypted and/or integrity protected. The functioning of the AVPF layer remains unchanged in SAVPF.

The AVPF profile derives from RFC 3550 [1] the (optional) use of the encryption prefix for RTCP. The encryption prefix MUST NOT be used within the SAVPF profile (it is not used in SAVP, as it is only applicable to the encryption method specified in [1]).

The SAVP part uses extra fields added to the end of RTP and RTCP packets and executes cryptographic transforms on (some of) the RTP/RTCP packet contents. This behavior remains unchanged in SAVPF. The average RTCP packet size calculation done by the AVPF layer for timing purposes MUST take into account the fields added by the SAVP layer.

The SRTP part becomes active only when the RTP or RTCP was scheduled by the "higher" AVPF layer or received from the transport protocol, irrespective of its timing and contents.

2.1. Packet Formats

AVPF defines extra packet formats to provide feedback information. Those extra packet formats defined in RFC 4585 [3] (and further ones defined elsewhere for use with AVPF) MAY be used with SAVPF.

SAVP defines a modified packet format for SRTP and SRTCP packets that essentially consists of the RTP/RTCP packet formats plus some trailing protocol fields for security purposes. For SAVPF, all RTCP packets MUST be encapsulated as defined in Section 3.4 of RFC 3711 [4].

2.2. Extensions

Extensions to AVPF RTCP feedback packets defined elsewhere MAY be used with the SAVPF profile provided that those extensions are in conformance with the extension rules of RFC 4585 [3].

Additional extensions (e.g., transforms) defined for SAVP following the rules of Section 6 of RFC 3711 [4] MAY also be used with the SAVPF profile. The overhead per RTCP packet depends on the extensions and transforms chosen. New extensions and transforms added in the future MAY introduce yet unknown further per-packet overhead.

Finally, further extensions specifically to SAVPF MAY be defined elsewhere.

2.3. Implications from Combining AVPF and SAVP

The AVPF profile aims at -- statistically -- allowing receivers to provide timely feedback to senders. The frequency at which receivers are, on average, allowed to send feedback information depends on the RTCP bandwidth, the group size, and the average size of an RTCP packet. SRTCP (see Section 3.4 of RFC 3711 [4]) adds extra fields (some of which are of configurable length) at the end of each RTCP packet that are probably at least some 10 to 20 bytes in size (14 bytes as default). Note that extensions and transforms defined in the future, as well as the configuration of each field length, MAY add greater overhead. By using SRTP, the average size of an RTCP packet will increase and thus reduce the frequency at which (timely) feedback can be provided. Application designers need to be aware of this, and take precautions so that the RTCP bandwidth shares are maintained. This MUST be done by adjusting the RTCP variable "avg_rtcp_size" to reflect the size of the SRTCP packets.

3. SDP Definitions

3.1. Profile Definition

The AV profiles defined in RFC 3551 [2], RFC 4585 [3], and RFC 3711 [4] are referred to as "AVP", "AVPF", and "SAVP", respectively, in the context of, e.g., the Session Description Protocol (SDP) [3]. The combined profile specified in this document is referred to as "SAVPF".

3.2. Attribute Definitions

SDP attributes for negotiating SAVP sessions are defined in RFC 4567 [7] and RFC 4568 [8]. Those attributes MAY also be used with SAVPF. The rules defined in [7] and [8] apply.

SDP attributes for negotiating AVPF sessions are defined in RFC 4585 [3]. Those attributes MAY also be used with SAVPF. The rules defined in [3] apply.

3.3. Profile Negotiation

Session descriptions for RTP sessions may be conveyed using protocols dedicated for multimedia communications such as the SDP offer/answer model (RFC 3264, [9]) used with the Session Initiation Protocol (SIP) [15], the Real Time Streaming Protocol (RTSP) [10], or the Session Announcement Protocol (SAP) [11], but may also be distributed using email, NetNews, web pages, etc.

The offer/answer model allows the resulting session parameters to be negotiated using the SDP attributes defined in RFC 4567 [7] and RFC 4568 [8]. In the following subsection, the negotiation process is described in terms of the offer/answer model.

Afterwards, the cases that do not use the offer/answer model are addressed: RTSP-specific negotiation support is provided by RFC 4567 [7] as discussed in Section 3.3.2, and support for SAP announcements (with no negotiation at all) is addressed in Section 3.3.3.

3.3.1. Offer/Answer-Based Negotiation of Session Descriptions

Negotiations (e.g., of RTP profiles, codecs, transport addresses, etc.) are carried out on a per-media session basis (e.g., per m= line in SDP). If negotiating one media session fails, others MAY still succeed.

Different RTP profiles MAY be used in different media sessions. For negotiation of a media description, the four profiles AVP, AVPF, SAVP, and SAVPF are mutually exclusive. Note, however, that SAVP and SAVPF entities MAY be mixed in a single RTP session (see Section 4). Also, the offer/answer mechanism MAY be used to offer alternatives for the same media session and allow the answerer to choose one of the profiles.

Provided that a mechanism for offering alternative security profiles becomes available (as is presently under development [14]), an offerer that is capable of supporting more than one of these profiles for a certain media session SHOULD always offer all alternatives acceptable in a certain situation. The alternatives SHOULD be listed in order of preference and the offerer SHOULD prefer secure profiles over non-secure ones. The offer SHOULD NOT include both a secure alternative (SAVP and SAVPF) and an insecure alternative (e.g., AVP and AVPF) in the same offer as this may enable bidding down and other attacks. Therefore, if both secure and non-secure RTP profiles are offered (e.g., for best-effort SRTP [14]), the negotiation signaling MUST be protected appropriately to avoid such attacks.

If an offer contains multiple alternative profiles, the answerer SHOULD prefer a secure profile (if supported) over non-secure ones. Among the secure or insecure profiles, the answerer SHOULD select the first acceptable alternative to respect the preference of the offerer.

If a media description in an offer uses SAVPF and the answerer does not support SAVPF, the media session MUST be rejected.

If a media description in an offer does not use SAVPF but the answerer wants to use SAVPF, the answerer MUST reject the media session. The answerer MAY provide a counter-offer with a media description indicating SAVPF in a subsequently initiated offer/answer exchange.

3.3.2. RTSP-Based Negotiation of Session Descriptions

RTSP [10] does not support the offer/answer model. However, RTSP supports exchanging media session parameters (including profile and address information) by means of the Transport header. SDP-based key management as defined in RFC 4567 [7] adds an RTSP header (KeyMgmt) to support conveying a key management protocol (including keying material).

The RTSP Transport header MAY be used to determine the profile for the media session. Conceptually, the rules defined in Section 3.3.1 apply accordingly. Detailed operation is as follows: An SDP description (e.g., retrieved from the RTSP server by means of DESCRIBE) contains the description of the media streams of the particular RTSP resource.

The RTSP client MUST select exactly one of the profiles per media stream it wants to receive. It MUST do so in the SETUP request. The RTSP client MUST indicate the chosen RTP profile by indicating the profile and the full server transport address (IP address and port number) in the Transport header included in the SETUP request. The RTSP server's response to the client's SETUP message MUST confirm this profile selection or refuse the SETUP request (the latter of which it should not do after offering the profiles in the first place).

> Note: To change any of the profiles in use, the client needs to tear down this media stream (and possibly the whole RTSP session) using the TEARDOWN method and re-establish it using SETUP. This may change as soon as media updating (similar to a SIP UPDATE or re-INVITE) becomes specified.

When using the SDP key management [7], the KeyMgmt header MUST be included in the appropriate RTSP messages if a secure profile is chosen. If different secure profiles are offered in the SDP description (e.g., SAVP and SAVPF) and different keying material is provided for these, after choosing one profile in the SETUP message, only the KeyMgmt header for the chosen one MUST be provided. The rules for matching KeyMgmt headers to media streams according to RFC 4567 [7] apply.

3.3.3. Announcing Session Descriptions

Protocols that do not allow negotiating session descriptions interactively (e.g., SAP [11], descriptions posted on a web page or sent by mail) pose the responsibility for adequate access to the media sessions on the initiator of a session.

The initiator SHOULD provide alternative session descriptions for multiple RTP profiles as far as acceptable to the application and the purpose of the session. If security is desired, SAVP may be offered as alternative to SAVPF -- but AVP or AVPF sessions SHOULD NOT be announced unless other security means not relying on SRTP are employed.

The SDP attributes defined in RFC 4567 [7] and RFC 4568 [8] may also be used for the security parameter distribution of announced session descriptions.

The security scheme description defined in RFC 4568 [8] requires a secure communications channel to prevent third parties from eavesdropping on the keying parameters and manipulation. Therefore, SAP security (as defined in RFC 2974 [11]), S/MIME [12], HTTPS [13], or other suitable mechanisms SHOULD be used for distributing or accessing these session descriptions.

3.3.4. Describing Alternative Session Profiles

SAVP and SAVPF entities MAY be mixed in the same RTP session (see also Section 4) and so MAY AVP and AVPF entities. Other combinations -- i.e., between secure and insecure profiles -- in the same RTP session are incompatible and MUST NOT be used together.

If negotiation between the involved peers is possible (as with the offer/answer model per Section 3.3.1 or RTSP per Section 3.3.2), alternative (secure and non-secure) profiles MAY be specified by one entity (e.g., the offerer) and a choice of one profile MUST be made by the other. If no such negotiation is possible (e.g., with SAP as per Section 3.3.3), incompatible profiles MUST NOT be specified as alternatives.

The negotiation of alternative profiles is for further study.

RTP profiles MAY be mixed arbitrarily across different RTP sessions.

3.4. Examples

This section includes examples for the use of SDP to negotiate the use of secure and non-secure profiles. Depending on what keying mechanism is being used and how it parameterized, the SDP messages typically require integrity protection and, for some mechanisms, will also need confidentiality protection. For example, one could say integrity protection is required for the a=fingerprint of Datagram Transport Layer Security - Secure Real-time Transport Protocol (DTLS-SRTP) [16], and confidentiality is required for RFC 4568 [8] (Security Descriptions) a=crypto.

Example 1: The following session description indicates a secure session made up from audio and dual tone multi-frequency (DTMF) for point-to-point communication in which the DTMF stream uses Generic NACKs. The key management protocol indicated is MIKEY. This session description (the offer) could be contained in a SIP INVITE or 200 OK message to indicate that its sender is capable of and willing to receive feedback for the DTMF stream it transmits. The corresponding answer may be carried in a 200 OK or an ACK. The parameters for the security protocol are negotiated as described by the SDP extensions defined in RFC 4567 [7].

```
v=0
o=alice 3203093520 3203093520 IN IP4 host.example.com
s=Media with feedback
t=0 0
c=IN IP4 host.example.com
m=audio 49170 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack
a=key-mgmt:mikey uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
```

Example 2: This example shows the same feedback parameters as example 1 but uses the secure descriptions syntax [8]. Note that the key part of the a=crypto attribute is not protected against eavesdropping and thus the session description needs to be exchanged over a secure communication channel.

```
v=0
o=alice 3203093520 3203093520 IN IP4 host.example.com
s=Media with feedback
t=0 0
c=IN IP4 host.example.com
m=audio 49170 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
```

```
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack
a=crypto:AES_CM_128_HMAC_SHA1_32
  inline:d/16/14/NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj/2^20/1
  :32
```

Example 3: This example is replicated from example 1 above, but shows the interaction between the offerer and the answerer in an offer/answer exchange, again using MIKEY to negotiate the keying material:

```
Offer:

v=0
o=alice 3203093520 3203093520 IN IP4 host.example.com
s=Media with feedback
t=0 0
c=IN IP4 host.example.com
a=key-mgmt:mikey uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
m=audio 49170 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack

Answer:

v=0
o=alice 3203093521 3203093521 IN IP4 host.another.example.com
s=Media with feedback
t=0 0
c=IN IP4 host.another.example.com
a=key-mgmt:mikey ushdgfdhgfuiweyfhjsgdkj2837do7eWsnDSJD...
m=audio 53012 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack
```

Example 4: This example shows the exchange for video streaming controlled via RTSP. A client acquires a media description from a server using DESCRIBE and obtains a static SDP description without any keying parameters, but the media description shows that both secure and non-secure media sessions using (S)AVPF are available. A mechanism that allows explicit identification of these alternatives (i.e., secure and non-secure sessions) in the session description is presently being defined [14]. The client then issues a SETUP request

and indicates its choice by including the respective profile in the Transport parameter. Furthermore, the client includes a KeyMgmt header to convey its security parameters, which is matched by a corresponding KeyMgmt header from the server in the response. Only a single media session is chosen so that the aggregate RTSP URI is sufficient for identification.

RTSP DESCRIBE request-response pair (optional):

```
DESCRIBE rtsp://movies.example.org/example RTSP/2.0
CSeq: 314
Accept: application/sdp

200 OK
CSeq: 314
Date: 25 Nov 2005 22:09:35 GMT
Content-Type: application/sdp
Content-Length: 316

v=0
o=alice 3203093520 3203093520 IN IP4 movies.example.com
s=Media with feedback
t=0 0
c=IN IP4 0.0.0.0
+-Alternative one-----------------+
|m=video 49170 RTP/SAVPF 96       |
|a=rtpmap:96 H263-2000/90000      |
|a=rtcp-fb:96 nack                |
+---------------------------------+
+-Alternative two-----------------+
|m=video 49172 RTP/AVPF 96        |
|a=rtpmap:96 H263-2000/90000      |
|a=rtcp-fb:96 nack                |
+---------------------------------+
```

RTSP SETUP request-response pair

```
SETUP rtsp://movies.example.org/example RTSP/2.0
CSeq: 315
Transport: RTP/SAVPF;unicast;dest_addr=":53012"/":53013"
KeyMgmt: prot=mikey;url="rtsp://movies.example.org/example";
         data="uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnD..."

200 OK
CSeq: 315
Date: 25 Nov 2005 22:09:36 GMT
Session: 4711
```

```
   Transport: RTP/SAVPF;unicast;dest_addr=":53012"/":53013";
              src_addr="192.0.2.15:60000"/"192.0.2.15:60001"
   KeyMgmt: prot=mikey;url="rtsp://movies.example.org/example";
            data="ushdgfdhgfuiweyfhjsgdkj2837do7eWsnDSJD..."
   Accept-Ranges: NPT, SMPTE
```

Example 5: The following session description indicates a multicast audio/video session (using PCMU for audio and either H.261 or H.263+) with the video source accepting Generic NACKs for both codecs and Reference Picture Selection for H.263. The parameters for the security protocol are negotiated as described by the SDP extensions defined in RFC 4567 [7], used at the session level. Such a description may have been conveyed using the Session Announcement Protocol (SAP).

```
   v=0
   o=alice 3203093520 3203093520 IN IP4 host.example.com
   s=Multicast video with feedback
   t=3203130148 3203137348
   a=key-mgmt:mikey uiSDF9sdhs7494ghsd/dhsoKkdOokdo7eWsnDSJD...
   m=audio 49170 RTP/SAVP 0
   c=IN IP4 224.2.1.183
   a=rtpmap:0 PCMU/8000
   m=video 51372 RTP/SAVPF 98 99
   c=IN IP4 224.2.1.184
   a=rtpmap:98 H263-1998/90000
   a=rtpmap:99 H261/90000
   a=rtcp-fb:* nack
   a=rtcp-fb:98 nack rpsi
```

4. Interworking of AVP, SAVP, AVPF, and SAVPF Entities

The SAVPF profile defined in this document is a combination of the SAVP profile [4] and the AVPF profile [3] (which in turn is an extension of the RTP profile as defined in RFC 3551 [2]).

SAVP and SAVPF use SRTP [4] to achieve security. AVP and AVPF use plain RTP [1] and hence do not provide security (unless external security mechanisms are applied as discussed in Section 9.1 of RFC 3550 [1]). SRTP and RTP are not meant to interoperate; the respective protocol entities are not supposed to be part of the same RTP session. Hence, AVP and AVPF on one side and SAVP and SAVPF on the other MUST NOT be mixed.

RTP entities using the SAVP and the SAVPF profiles MAY be mixed in a single RTP session. The interworking considerations defined in Section 5 of RFC 4585 [3] apply.

5. Security Considerations

The SAVPF profile inherits its security properties from the SAVP profile; therefore, it is subject to the security considerations discussed in RFC 3711 [4]. When compared to SAVP, the SAVPF profile does not add or take away any security services.

There is a desire to support security for media streams and, at the same time, for backward compatibility with non-SAVP(F) nodes.

Application designers should be aware that security SHOULD NOT be traded for interoperability. If information is to be distributed to closed groups (i.e., confidentially protected), it is RECOMMENDED not to offer alternatives for a media session other than SAVP and SAVPF as described in Sections 3.3 and 3.4, unless other security mechanisms will be used, e.g., the ones described in Section 9.1 of RFC 3550 [1]. Similarly, if integrity protection is considered important, it is RECOMMENDED not to offer the alternatives other than SAVP and SAVPF, unless other mechanisms are known to be in place that can guarantee it, e.g., lower-layer mechanisms as described in Section 9 of RFC 3550 [1].

Offering secure and insecure profiles simultaneously may open to bidding down attacks. Therefore, such a mix of profile offer SHOULD NOT be made.

Note that the rules for sharing master keys apply as described in RFC 3711 [4] (e.g., Section 9.1). In particular, the same rules for avoiding the two-time pad (keystream reuse) apply: a master key MUST NOT be shared among different RTP sessions unless the SSRCs used are unique across all the RTP streams of the RTP sessions that share the same master key.

When 2^48 SRTP packets or 2^31 SRTCP packets have been secured with the same key (whichever occurs before), the key management MUST be called to provide new master key(s) (previously stored and used keys MUST NOT be used again), or the session MUST be terminated.

Different media sessions may use a mix of different profiles, particularly including a secure profile and an insecure profile. However, mixing secure and insecure media sessions may reveal information to third parties and thus the decision to do so MUST be in line with a local security policy. For example, the local policy MUST specify whether it is acceptable to have, e.g., the audio stream not secured and the related video secured.

The security considerations in RFC 4585 [3] are valid, too. Note in particular, applying the SAVPF profile implies mandatory integrity protection on RTCP. While this solves the problem of false packets from members not belonging to the group, it does not solve the issues related to a malicious member acting improperly.

6. IANA Considerations

The following contact information shall be used for all registrations included here:

Contact: Joerg Ott
mail: jo@acm.org
tel: +358-9-451-2460

The secure RTP feedback profile, as a combination of Secure RTP and the feedback profile, has been registered for the Session Description Protocol (specifically the type "proto"): "RTP/SAVPF".

SDP Protocol ("proto"):

Name:	RTP/SAVPF
Long form:	Secure RTP Profile with RTCP-based Feedback
Type of name:	proto
Type of attribute:	Media level only
Purpose:	RFC 5124
Reference:	RFC 5124

All the SDP attributes defined for RTP/SAVP and RTP/AVPF are valid for RTP/SAVPF, too.

7. Acknowledgements

This document is a product of the Audio-Visual Transport (AVT) Working Group of the IETF. The authors would like to thank Magnus Westerlund, Colin Perkins, and Cullen Jennings for their comments.

8. References

8.1. Normative References

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

[2] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, July 2003.

[3] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585, July 2006.

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

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

[6] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[7] Arkko, J., Lindholm, F., Naslund, M., Norrman, K., and E. Carrara, "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)", RFC 4567, July 2006.

[8] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, July 2006.

[9] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[10] Schulzrinne, H., Rao, A., and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, April 1998.

8.2. Informative References

[11] Handley, M., Perkins, C., and E. Whelan, "Session Announcement Protocol", RFC 2974, October 2000.

[12] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[13] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[14] Andreasen, F., "SDP Capability Negotiation", Work in Progress, December 2007.

[15] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[16] McGrew, D. and Rescorla, E., "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)", Work in Progress, November 2007.

Authors' Addresses

Joerg Ott
Helsinki University of Technology
Otakaari 5A
FI-02150 Espoo
Finland

EMail: jo@comnet.tkk.fi
Phone: +358-9-451-2460

Elisabetta Carrara
Royal Institute of Technology
Stockholm
Sweden

EMail: carrara@kth.se

Full Copyright Statement

Intellectual Property