              Why RTP Does Not Mandate a Single Security Mechanism
                  draft-ietf-avt-srtp-not-mandatory-06.txt

Abstract

   This memo discusses the problem of securing real-time multimedia
   sessions, and explains why the Real-time Transport Protocol (RTP),
   and the associated RTP control protocol (RTCP), do not mandate a
   single media security mechanism.

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on January 1, 2011.

Table of Contents

1. Introduction

   The Real-time Transport Protocol (RTP) [RFC3550] is widely used for
   voice over IP, Internet television, video conferencing, and various
   other real-time and streaming media applications. Despite this, the
   base RTP specification provides very limited options for media
   security, and defines no standard key exchange mechanism. Rather, a
   number of extensions are defined to provide confidentiality and
   authentication of RTP media streams and RTCP control messages, and to
   exchange security keys. This memo outlines why it is appropriate
   that multiple extension mechanisms are defined, rather than mandating
   a single security and keying mechanism.

   This memo provides information for the community; it does not specify
   a standard of any kind.

   The structure of this memo is as follows. Section 2 describes the
   scenarios in which RTP is deployed. Following this, Section 3
   outlines the implications of this range of scenarios for media
   confidentially and authentication, and Section 4 outlines the
   implications for key exchange. Section 5 outlines how the RTP
   framework meets the requirement of BCP 61. Section 6 then concludes
   and gives some recommendations.

2. RTP Applications and Deployment Scenarios

   The range of application and deployment scenarios where RTP has been
   used includes, but is not limited to, the following:

   o Point-to-point voice telephony (fixed and wireless networks)

   o Point-to-point video conferencing

   o Centralised group video conferencing with a multipoint conference
      unit (MCU)

   o Any Source Multicast video conferencing (light-weight sessions;
      Mbone conferencing)

   o Point-to-point streaming audio and/or video

   o Source-specific multicast (SSM) streaming to large group (IPTV and
      3GPP Multimedia Broadcast Multicast Service (MBMS) [MBMS])

   o Replicated unicast streaming to a group

o Interconnecting components in music production studios and video
   editing suites

o Interconnecting components of distributed simulation systems

o Streaming real-time sensor data

As can be seen, these scenarios vary from point-to-point to very
large multicast groups, from interactive to non-interactive, and from
low bandwidth (kilobits per second) to very high bandwidth (multiple
gigabits per second). While most of these applications run over UDP
[RFC0768], some use TCP [RFC0793], [RFC4614] or DCCP [RFC4340] as
their underlying transport. Some run on highly reliable optical
networks, others use low rate unreliable wireless networks. Some
applications of RTP operate entirely within a single trust domain,
others are inter-domain, with untrusted (and potentially unknown)
users. The range of scenarios is wide, and growing both in number
and in heterogeneity.

3. Implications for RTP Security

The wide range of application scenarios where RTP is used has led to
the development of multiple solutions for securing RTP media streams
and RTCP control messages, considering different requirements.
Perhaps the most widely applicable of these solutions is the Secure
RTP (SRTP) framework [RFC3711]. This is an application-level media
security solution, encrypting the media payload data (but not the RTP
headers) to provide some degree of confidentiality, and providing
optional source origin authentication. It was carefully designed to
be both low overhead, and to support the group communication features
of RTP, across a range of networks.

SRTP is not the only media security solution in use, however, and
alternatives are more appropriate for some scenarios. For example,
many client-server streaming media applications can run over a single
TCP connection, multiplexing media data with control information on
that connection (RTSP [I-D.ietf-mmusic-rfc2326bis] is a widely used
example of such a protocol). The natural way to provide media
security for such client-server media applications is to use TLS
[RFC5246] to protect the TCP connection, sending the RTP media data
over the TLS connection. Using the SRTP framework in addition to TLS
is unnecessary, and would result in double encryption of the media,
and SRTP cannot be used instead of TLS since it is RTP-specific, and
so cannot protect the control traffic.

Other RTP use cases work over networks which provide security at the
network layer, using IPsec. For example, certain 3GPP networks need

IPsec security associations for other purposes, and can reuse those
to secure the RTP session [3GPP.33.210]. SRTP is, again, unnecessary
in such environments, and its use would only introduce overhead for
no gain.

For some applications it is sufficient to protect the RTP payload
data while leaving RTP, transport, and network layer headers
unprotected. An example of this is RTP broadcast over DVB-H
[ETSI.TS.102.474], where one mode of operation uses ISMAcryp
(http://www.isma.tv/specs/ISMA_E&Aspec2.0.pdf) to encrypt the RTP
payload data only.

Finally, the link layer may be secure, and it may be known that the
RTP media data is constrained to that single link (for example, when
operating in a studio environment, with physical link security). An
environment like this is inherently constrained, but might avoid the
need for application, transport, or network layer media security.

All these are application scenarios where RTP has seen commercial
deployment. Other use case also exist, with additional requirements.
There is no media security protocol that is appropriate for all these
environments. Accordingly, multiple RTP media security protocols can
be expected to remain in wide use.

4. Implications for Key Management

With such a diverse range of use cases come a range of different
protocols for RTP session establishment. Mechanisms used to provide
security keying for these different session establishment protocols
can basically be put into two categories: inband and out-of-band in
relation to the session establishment mechanism. The requirements
for these solutions are highly varying. Thus a wide range of
solutions have been developed in this space:

o A common use case for RTP is probably point-to-point voice calls
   or centralised group conferences, negotiated using SIP [RFC3261]
   with the SDP offer/answer model [RFC3264], operating on a trusted
   infrastructure. In such environments, SDP security descriptions
   [RFC4568] or the MIKEY [RFC4567] protocol are appropriate keying
   mechanisms, piggybacked onto the SDP [RFC4566] exchange. The
   infrastructure may be secured by protecting the SIP exchange using
   TLS or S/MIME, for example [RFC3261]. Protocols such as DTLS
   [RFC5764] or ZRTP [I-D.zimmermann-avt-zrtp] may also be
   appropriate in such environments.

o Point-to-point RTP sessions may be negotiated using SIP with the
   offer/answer model, but operating over a network with untrusted

infrastructure. In such environments, the key management protocol
is run on the media path, bypassing the untrusted infrastructure.
Protocols such as DTLS [RFC5764] or ZRTP [I-D.zimmermann-avt-zrtp]
are useful here.

o For point-to-point client-server streaming of RTP over RTSP, a TLS
   association is appropriate to manage keying material, in much the
   same manner as would be used to secure an HTTP session.

o A session description may be sent by email, secured using S/MIME
   or PGP, or retrieved from a web page, using HTTP with TLS.

o A session description may be distributed to a multicast group
   using SAP or FLUTE secured with S/MIME.

o A session description may be distributed using the Open Mobile
   Alliance DRM key management specification [OMA-DRM] when using a
   point-to-point streaming session setup with RTSP in the 3GPP PSS
   environment [PSS].

o In the 3GPP Multimedia Broadcast Multicast Service (MBMS) system,
   HTTP and MIKEY are used for key management [MBMS-SEC].

A more detailed survey of requirements for media security management
protocols can be found in [RFC5479]. As can be seen, the range of
use cases is wide, and there is no single protocol that is
appropriate for all scenarios. These solutions have been further
diversified by the existence of infrastructure elements such as
authentication solutions that are tied into the key manangement.

5. On the Requirement for Strong Security in IETF protocols

BCP 61 [RFC3365] puts a requirement on IETF protocols to provide
strong, mandatory to implement, security solutions. This is actually
quite a difficult requirement for any type of framework protocol,
like RTP, since one can never know all the deployment scenarios, and
if they are covered by the security solution. It would clearly be
desirable if a single media security solution and a single key
management solution could be developed, satisfying the range of use
cases for RTP. The authors are not aware of any such solution,
however, and it is not clear that any single solution can be
developed.

For a framework protocol it appears that the only sensible solution
to the requirement of BCP 61 is to develop or use security building
blocks, like SRTP, SDP security descriptions [RFC4568], MIKEY, DTLS,
or IPsec, to provide the basic security services of authorization,

data integrity protection and date confidentiality protection. When
new usages of the RTP framework arise, one needs to analyze the
situation, to determine if the existing building blocks satisfy the
requirements. If not, it is necessary to develop new security
building blocks.

When it comes to fulfilling the "MUST Implement" strong security for
a specific application, it will fall on that application to actually
consider what building blocks it is required to support. To maximize
interoperability it is desirable if certain applications, or classes
of application with similar requirements, agree on what data security
mechanisms and key-management should be used. If such agreement is
not possible, there will be increased cost, either in the lack of
interoperability, or in the need to implement more solutions.
Unfortunately this situation, if not handled reasonably well, can
result in a failure to satisfy the requirement of providing the users
with an option of turning on strong security when desired.

6. Conclusions

As discussed earlier it appears that a single solution can't be
designed to meet the diverse requirements. In the absence of such a
solution, it is hoped that this memo explains why SRTP is not
mandatory as the media security solution for RTP-based systems, and
why we can expect multiple key management solutions for systems using
RTP.

It is important for any RTP-based application to consider how it
meets the security requirements. This will require some analysis to
determine these requirements, followed by the selection of a
mandatory to implement solution, or in exceptional scenarios several
solutions, including the desired RTP traffic protection and key-
management. SRTP is a preferred solution for the protection of the
RTP traffic in those use cases where it is applicable. It is out of
scope for this memo to recommend a preferred key management solution.

7. Security Considerations

This entire memo is about security.

8. IANA Considerations

No IANA actions are required.

9. Acknowledgements

   Thanks to Ralph Blom, Hannes Tschofenig, Dan York, Alfred Hoenes,
   Martin Ellis, Ali Begen, and Keith Drage for their feedback.

10. Informative References

   [3GPP.33.210]
               3GPP, "IP network layer security", 3GPP TS 33.210.

   [ETSI.TS.102.474]
               ETSI, "Digital Video Broadcasting (DVB); IP Datacast over
               DVB-H: Service Purchase and Protection", ETSI TS 102 474,
               November 2007.

   [I-D.ietf-mmusic-rfc2326bis]
               Schulzrinne, H., Rao, A., Lanphier, R., Westerlund, M.,
               and M. Stiemerling, "Real Time Streaming Protocol 2.0
               (RTSP)", draft-ietf-mmusic-rfc2326bis-23 (work in
               progress), March 2010.

   [I-D.zimmermann-avt-zrtp]
               Zimmermann, P., Johnston, A., and J. Callas, "ZRTP: Media
               Path Key Agreement for Unicast Secure RTP",
               draft-zimmermann-avt-zrtp-22 (work in progress),
               June 2010.

   [MBMS]   3GPP, "Multimedia Broadcast/Multicast Service (MBMS);
               Protocols and codecs TS 26.346".

   [MBMS-SEC]
               3GPP, "Security of Multimedia Broadcast/Multicast Service
               (MBMS) TS 33.246".

   [OMA-DRM]   Open Mobile Alliance, "DRM Specification 2.0".

   [PSS]   3GPP, "Transparent end-to-end Packet-switched Streaming
               Service (PSS); Protocols and codecs TS 26.234".

   [RFC0768]   Postel, J., "User Datagram Protocol", STD 6, RFC 768,
               August 1980.

   [RFC0793]   Postel, J., "Transmission Control Protocol", STD 7,
               RFC 793, September 1981.

   [RFC3261]   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.

   [RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model
              with Session Description Protocol (SDP)", RFC 3264,
              June 2002.

   [RFC3365] Schiller, J., "Strong Security Requirements for Internet
              Engineering Task Force Standard Protocols", BCP 61,
              RFC 3365, August 2002.

   [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.

   [RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram
              Congestion Control Protocol (DCCP)", RFC 4340, March 2006.

   [RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
              Description Protocol", RFC 4566, July 2006.

   [RFC4567] 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.

   [RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session
              Description Protocol (SDP) Security Descriptions for Media
              Streams", RFC 4568, July 2006.

   [RFC4614] Duke, M., Braden, R., Eddy, W., and E. Blanton, "A Roadmap
              for Transmission Control Protocol (TCP) Specification
              Documents", RFC 4614, September 2006.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246, August 2008.

   [RFC5479] Wing, D., Fries, S., Tschofenig, H., and F. Audet,
              "Requirements and Analysis of Media Security Management
              Protocols", RFC 5479, April 2009.

   [RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer
              Security (DTLS) Extension to Establish Keys for the Secure
              Real-time Transport Protocol (SRTP)", RFC 5764, May 2010.

Authors' Addresses

    Colin Perkins
    University of Glasgow
    Department of Computing Science
    Glasgow G12 8QQ
    UK

    Email: csp@csperkins.org

    Magnus Westerlund
    Ericsson
    Farogatan 6
    Kista SE-164 80
    Sweden

    Email: magnus.westerlund@ericsson.com