Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2012

C. Perkins
University of Glasgow
M. Westerlund
Ericsson

October 31, 2011

Why RTP Does Not Mandate a Single Security Mechanism
draft-ietf-avt-srtp-not-mandatory-08.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. It also discusses how applications using RTP can meet the goals of BCP 61 to have strong and mandatory to implement security.

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.

The consensus for Strong Security Requirements for IETF Standard Protocols (BCP61) [RFC3365] describes the Danvers Doctrine, which states that:

> "The solution is that we MUST implement strong security in all protocols to provide for the all too frequent day when the protocol comes into widespread use in the global Internet."

BCP 61 also discusses that security must be implemented, and makes the following statement:

> "However security must be a MUST IMPLEMENT so that end users will have the option of enabling it when the situation calls for it."

This IETF consensus provides a clear challange for RTP security, due to the heterogenous scenarios in which RTP can be used, and the wide choice of security mechanisms available. This memo describes how RTP based applications, or classes of applications, can best meet the security goals of BCP 61.

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 a number of 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 can meet 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:

- Point-to-point voice telephony (fixed and wireless networks)
- Point-to-point voice and video conferencing
- Centralised group video conferencing with a multipoint conference unit (MCU)
- Any Source Multicast video conferencing (light-weight sessions; Mbone conferencing)
- Point-to-point streaming audio and/or video
- Source-specific multicast (SSM) streaming to large group (IPTV and 3GPP Multimedia Broadcast Multicast Service (MBMS) [MBMS])
- Replicated unicast streaming to a group
- Interconnecting components in music production studios and video editing suites
- Interconnecting components of distributed simulation systems
- 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). One 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 [TS-33210]. 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 ISMA Cryp 2.0 [ISMA] to encrypt the RTP payload data only.

All these are application scenarios where RTP has seen commercial deployment. Other use cases exist, with additional requirements. For example, if the media transport is done over UDP [RFC0768], DCCP [RFC4340] or SCTP [RFC4960], then using DTLS [RFC4347] to protect the whole RTP packets is an option. 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:

- 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 [RFC3830] protocol using the Key Management Extensions for SDP [RFC4567], are appropriate keying mechanisms, where the keying messages/material are embedded in the SDP [RFC4566] exchange. The infrastructure may be secured by protecting the SDP exchange in SIP using TLS or S/MIME, for example [RFC3261]. Protocols such as DTLS-SRTP [RFC5764] or ZRTP [RFC6189] are also appropriate in such environments.

- 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 can be run on the media path, bypassing the untrusted infrastructure. Protocols such as DTLS-SRTP [RFC5764] or ZRTP [RFC6189] are useful here, as are inband mechanism that protect the keying material such as MIKEY [RFC3830] using the Key Management Extensions for SDP [RFC4567]. It should be noted that the end-points for all the above mechanisms must prevent total downgrade to no security for the RTP media streams.

- 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. But also using SRTP with DTLS-SRTP keying or DTLS are appropriate choices.

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

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

- 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].

- 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 management.

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 solution. This is actually quite a difficult requirement for any type of framework protocol like RTP, or for that matter the Reliable Multicast Transport suite [RFC3048], 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 believe it is unlikely 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, MIKEY, DTLS, DTLS-SRTP, 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, or class of applications, 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.

The IETF needs to perform this selection of security building blocks whenever it is possible. This can be done if the application, or class of applications, is being specified within the IETF, or wich a scope where the IETF can take the role to provide a security profile. However, it is clear that many applications, or classes of application, are specified outside the scope and influence of the IETF. In those case we can't do other than strongly recommend these

organizations perform a security analysis, taking into account other applications, to try to maximize the security and interoperability.

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 very 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. When defining applications or protocols using RTP within the IETF, the responsibility for fulfilling the BCP 61 requirements will fall onto the developers of these applications. IETF also should be open to help other standards bodies by defining security profiles suitable for classes of applications.

Anyone defining an RTP based application needs to take care to consider how to fulfill its security goals and specify which mechanisms that are to be implemented. In that work interoperability with similar applications should be considered, so that when such applications becomes desirable to interconnect those applications, their security solutions are compatible and will not require additional implementation or costly gateways that also reduce security by forcing a trusted third party.

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 in general. The authors do note that DTLS-SRTP was developed in the IETF to meet the goals of point to point media sessions established by SIP.

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

[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-28 (work in progress), October 2011.

[ISMA] Internet Streaming Media Alliance, "Encryption and Authentication Version 2.0", November 2007.

[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.

[RFC3048] Whetten, B., Vicisano, L., Kermode, R., Handley, M., Floyd, S., and M. Luby, "Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer", RFC 3048, January 2001.

[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.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

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

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 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.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[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.

[RFC6189] Zimmermann, P., Johnston, A., and J. Callas, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", RFC 6189, April 2011.

[TS-33210] 3GPP, "IP network layer security", 3GPP TS 33.210.

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