Workgroup: Payload Working Group
Internet-Draft: draft-ietf-avtcore-rtp-scip-09
Published: 13 February 2024
Intended Status: Standards Track
Expires: 16 August 2024
Authors: D. Hanson
General Dynamics Mission Systems, Inc.
M. Faller
General Dynamics Mission Systems, Inc.
K. Maver
General Dynamics Mission Systems, Inc.

RTP Payload Format for the Secure Communication Interoperability Protocol (SCIP) Codec

Abstract

This document describes the RTP payload format of the Secure Communication Interoperability Protocol (SCIP). SCIP is an application layer protocol that provides end-to-end capability exchange, packetization/de-packetization of media, reliable transport, and payload encryption.

SCIP handles packetization/de-packetization of the encrypted media and acts as a tunneling protocol, treating SCIP payloads as opaque octets to be encapsulated within RTP payloads prior to transmission or decapsulated on reception. SCIP payloads are sized to fit within the maximum transmission unit (MTU) when transported over RTP thereby avoiding fragmentation.

SCIP transmits encrypted traffic and does not require the use of Secure RTP (SRTP) for payload protection. SCIP also provides for reliable transport at the application layer, so it is not necessary to negotiate RTCP retransmission capabilities.

To establish reliable communications using SCIP over RTP, it is important that middle boxes avoid parsing or modifying SCIP payloads. Because SCIP payloads are confidentiality and integrity protected and are only decipherable by the originating and receiving SCIP devices, modification of the payload by middle boxes would be detected as an integrity failure in SCIP devices, resulting in retransmission and/or communication failure. Middle boxes do not need to parse the SCIP payloads to correctly transport them. Not only is parsing unnecessary to tunnel/detunnel SCIP within RTP, but the parsing and filtering of SCIP payloads by middle boxes would likely lead to ossification of the evolving SCIP protocol.

Status of This Memo

Copyright Notice

Table of Contents

1. Key Points

*SCIP is an application layer protocol that uses RTP as a transport. This document defines the SCIP media subtypes to be listed in the Session Description Protocol (SDP) and only requires a basic RTP transport channel for SCIP payloads. This basic transport channel is comparable to [RFC4040] Clearmode.

*SCIP is designed to be network agnostic. It can operate over any digital link, including non-IP modem-based PSTN and ISDN. The SCIP media subtypes listed in this document were developed for SCIP to operate over RTP.

*SCIP handles packetization/de-packetization of payloads by producing encrypted media packets that are not greater than the MTU size. The SCIP payload is opaque to the network, therefore, SCIP functions as a tunneling protocol for the encrypted media, without the need for middle boxes to parse SCIP payloads. Since SCIP payloads are integrity protected, modification of the SCIP payload is detected as an integrity violation by SCIP endpoints leading to communication failure.

*SCIP includes built-in mechanisms that negotiate protocol message versions and capabilities. To avoid SCIP protocol ossification (as described in [RFC9170]), it is important for middle boxes to not attempt parsing of the SCIP payload. As described in this document, such parsing serves no useful purpose.

2. Introduction

The purpose of this document is to provide enough information to enable SCIP payloads to be transported through the network without modification or filtering. The document provides a reference for network security policymakers; network equipment OEMs, administrators, and architects; procurement personnel; and government agency and commercial industry representatives.

The document details usage of the "audio/scip" and "video/scip" pseudo-codecs [AUDIOSCIP], [VIDEOSCIP] as a secure session establishment protocol and media transport protocol over RTP. It discusses (1) how encrypted audio and video codec payloads are transported over RTP; (2) the IP network layer not implementing SCIP as a protocol since SCIP operates at the application layer in endpoints; (3) the IP network layer enabling SCIP traffic to

transparently pass through the network; (4) network devices not recognizing SCIP, and thus removing the scip codecs from the SDP media payload declaration before forwarding to the next network node; and finally, (5) SCIP endpoint devices not operating on networks due to the scip media subtype removal from the SDP media payload declaration.

The United States, along with its NATO Partners, have implemented SCIP in secure voice, video, and data products operating on commercial, private, and tactical IP networks worldwide using the scip media subtype. The SCIP data traversing the network is encrypted, and network equipment in-line with the session cannot interpret the traffic stream in any way. SCIP-based RTP traffic is opaque and can vary significantly in structure and frequency making traffic profiling not possible. Also, as the SCIP protocol continues to evolve independently of this document, any network device that attempts to filter traffic (e.g., deep packet inspection) may cause unintended consequences in the future when changes to the SCIP traffic may not be recognized by the network device.

The SCIP protocol defined in SCIP-210 [SCIP210] includes built-in support for packetization/de-packetization, retransmission, capability exchange, version negotiation, and payload encryption. Since the traffic is encrypted, neither the RTP transport nor middle boxes can usefully parse or modify SCIP payloads; modifications are detected as integrity violations resulting in retransmission, and eventually, communication failure.

Because knowledge of the SCIP payload format is not needed to transport SCIP signaling or media through middle boxes, SCIP-210 represents an informative reference. While older versions of the SCIP-210 specification are publicly available, the authors strongly encourage network implementers to treat SCIP payloads as opaque octets. When handled correctly, such treatment does not require referring to SCIP-210, and any assumptions about the format of SCIP messages defined in SCIP-210 are likely to lead to protocol ossification and communication failures as the protocol evolves.

Note: The IETF has not conducted a security review of SCIP and therefore has not verified the claims contained in this document.

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Best current practices for writing an RTP payload format specification were followed [RFC2736] [RFC8088].

When referring to the Secure Communication Interoperability Protocol, the uppercase acronym "SCIP" is used. When referring to the media subtype scip, lowercase "scip" is used.

2.2. Abbreviations

The following abbreviations are used in this document.

AVP: Audio/Video Profile
AVPF: Audio/Video Profile Feedback
ICWG: Interoperability Control Working Group
IICWG: International Interoperability Control Working Group
NATO: North Atlantic Treaty Organization
OEM: Original Equipment Manufacturer
SAVP: Secure Audio/Video Profile
SAVPF: Secure Audio/Video Profile Feedback
SCIP: Secure Communication Interoperability Protocol
SDP: Session Description Protocol
SRTP: Secure Real-Time Transport Protocol
STANAG: Standardization Agreement

3. Background

The Secure Communication Interoperability Protocol (SCIP) allows the negotiation of several voice, data, and video applications using various cryptographic suites. SCIP also provides several important characteristics that have led to its broad acceptance as a secure communications protocol.

SCIP began in the United States as the Future Narrowband Digital Terminal (FNBDT) Protocol in the late 1990s. A combined U.S. Department of Defense and vendor consortium formed a governing organization named the Interoperability Control Working Group (ICWG) to manage the protocol. In time, the group expanded to include NATO, NATO partners and European vendors under the name International Interoperability Control Working Group (IICWG), which was later renamed the SCIP Working Group.

First generation SCIP devices operated on circuit-switched networks. SCIP was then expanded to radio and IP networks. The scip media subtype transports SCIP secure session establishment signaling and secure application traffic. The built-in negotiation and flexibility provided by the SCIP protocols make it a natural choice for many scenarios that require various secure applications and associated encryption suites. SCIP has been adopted by NATO in STANAG 5068. SCIP standards are currently available to participating government/ military communities and select OEMs of equipment that support SCIP.

However, SCIP must operate over global networks (including private and commercial networks). Without access to necessary information to support SCIP, some networks may not support the SCIP media subtypes. Issues may occur simply because information is not as readily available to OEMs, network administrators, and network architects.

This document provides essential information about audio/scip and video/scip media subtypes that enables network equipment manufacturers to include settings for "scip" as a known audio and video media subtype in their equipment. This enables network administrators to define and implement a compatible security policy which includes audio and video media subtypes "audio/scip" and "video/scip", respectively, as permitted codecs on the network.

All current IP-based SCIP endpoints implement "scip" as a media subtype. Registration of scip as a media subtype provides a common reference for network equipment manufacturers to recognize SCIP in an SDP payload declaration.

4. Payload Format

The "scip" media subtype indicates support for and identifies SCIP traffic that is being transported over RTP. Transcoding, lossy compression, or other data modifications MUST NOT be performed by the network on the SCIP RTP payload. The audio/scip and video/scip media subtype data streams within the network, including the VoIP network, MUST be a transparent relay and be treated as "clear-channel data", similar to the Clearmode media subtype defined by [RFC4040].

RFC 4040 is referenced because Clearmode does not define specific RTP payload content, packet size, or packet intervals, but rather enables Clearmode devices to signal that they support a compatible mode of operation and defines a transparent channel on which devices may communicate. This document takes a similar approach. Network devices that implement support for SCIP need to enable SCIP endpoints to signal that they support SCIP and provide a transparent channel on which SCIP endpoints may communicate.

SCIP is an application layer protocol that is defined in SCIP-210. The SCIP traffic consists of encrypted SCIP control messages and codec data. The payload size and interval will vary considerably depending on the state of the SCIP protocol within the SCIP device.

Figure 1 below illustrates the RTP payload format for SCIP.

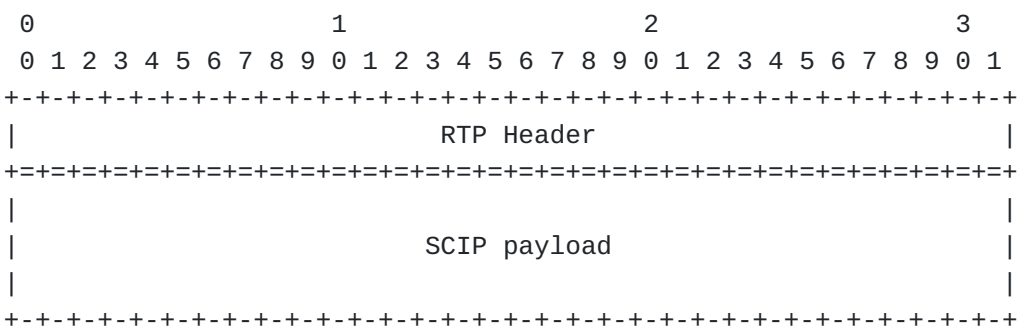

Figure 1: SCIP RTP Payload Format

The SCIP codec produces an encrypted bitstream that is transported over RTP. Unlike other codecs, SCIP does not have its own upper layer syntax (e.g., no Network Adaptation Layer (NAL) units), but rather encrypts the output of the audio/video codecs that it uses (e.g., G.729D, H.264 [RFC6184], etc.). SCIP achieves this by encapsulating the encrypted codec output that has been previously formatted according to the relevant RTP payload specification for that codec. SCIP endpoints MAY employ mechanisms, such as Inter-media RTP Synchronization as described in [RFC8088] Section 3.3.4, to synchronize audio/scip and video/scip streams.

Figure 2 below illustrates notionally how codec packets and SCIP control messages are packetized for transmission over RTP.

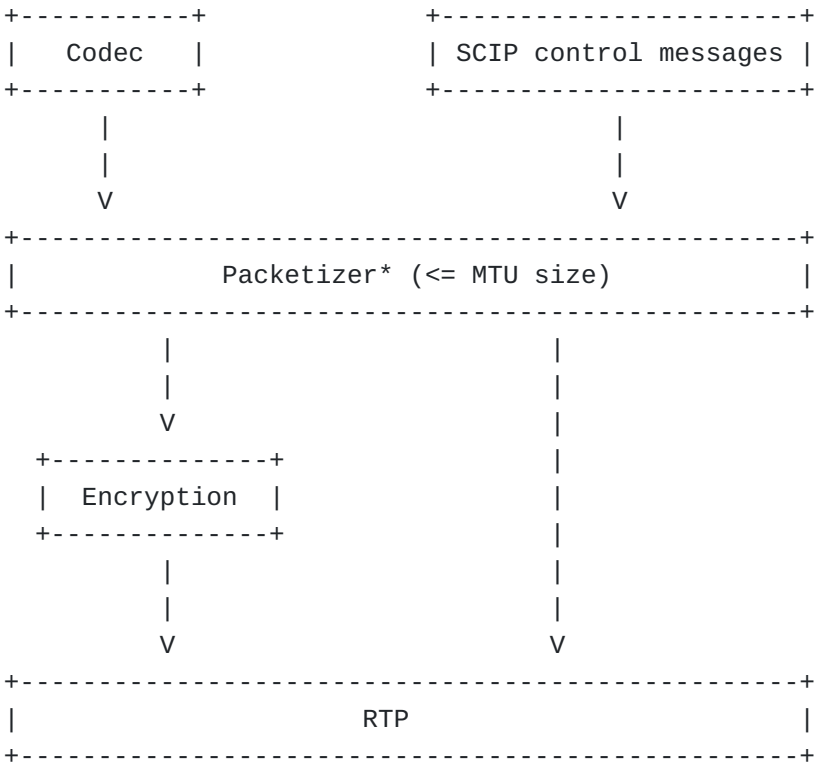

Figure 2: SCIP RTP Architecture

* Packetizer: The SCIP application layer will ensure that all traffic sent to the RTP layer will not exceed the MTU size. The receiving SCIP RTP layer will handle packet identification, ordering, and reassembly. When required, the SCIP application layer handles error detection and retransmission.

As described above, the SCIP RTP payload format is variable and cannot be described in specificity in this document. Details can be found in SCIP-210. SCIP will continue to evolve and as such the SCIP RTP traffic MUST NOT be filtered by network devices based upon what currently is observed or documented. The focus of this document is for network devices to consider the SCIP RTP payload as opaque and allow it to traverse the network. Network devices MUST NOT modify SCIP RTP packets.

4.1. RTP Header Fields

The SCIP RTP header fields SHALL conform to RFC 3550.

SCIP traffic may be continuous or discontinuous. The Timestamp field MUST increment based on the sampling clock for discontinuous transmission as described in [RFC3550], Section 5.1. The Timestamp field for continuous transmission applications is dependent on the sampling rate of the media as specified in the media subtype's specification (e.g., MELPe). Note that during a SCIP session, both discontinuous and continuous traffic are highly probable.

The Marker bit SHALL be set to zero for discontinuous traffic. The Marker bit for continuous traffic is based on the underlying media subtype specification. The underlying media is opaque within SCIP RTP packets.

4.2. Congestion Control Considerations

The bitrate of SCIP may be adjusted depending on the capability of the underlying codec (such as MELPe [RFC8130], G.729D [RFC3551], etc.). The number of encoded audio frames per packet may also be adjusted to control congestion. Discontinuous transmission may also be used if supported by the underlying codec.

Since UDP does not provide congestion control, applications that use RTP over UDP SHOULD implement their own congestion control above the UDP layer [RFC8085] and MAY also implement a transport circuit breaker [RFC8083]. Work in the RTP Media Congestion Avoidance Techniques (RMCAT) working group [RMCAT] describes the interactions and conceptual interfaces necessary between the application components that relate to congestion control, including the RTP layer, the higher-level media codec control layer, and the lower-

level transport interface, as well as components dedicated to congestion control functions.

Use of the packet loss feedback mechanisms in AVPF [RFC4585] and SAVPF [RFC5124] are OPTIONAL because SCIP itself manages retransmissions of some errored or lost packets. Specifically, the Payload-Specific Feedback Messages defined in RFC 4585 section 6.3 are OPTIONAL when transporting video data.

4.3. Use of Augmented RTP Transport Protocols with SCIP

The SCIP application layer protocol uses RTP as a basic transport for the audio/scip and video/scip payloads. Additional RTP transport protocols that do not modify the SCIP payload are considered OPTIONAL in this document and are discretionary for a SCIP device vendor to implement. Some examples include but are not limited to:

- *RTP Payload Format for Generic Forward Error Correction [RFC5109]
- *Multiplexing RTP Data and Control Packets on a Single Port [RFC5761]
- *Symmetric RTP/RTP Control Protocol (RTCP) [RFC4961]
- *Negotiating Media Multiplexing Using the Session Description Protocol (BUNDLE) [RFC9143]

5. Payload Format Parameters

The SCIP RTP payload format is identified using the scip media subtype, which is registered in accordance with [RFC4855] and per the media type registration template form [RFC6838]. A clock rate of 8000 Hz SHALL be used for "audio/scip". A clock rate of 90000 Hz SHALL be used for "video/scip".

5.1. Media Subtype "audio/scip"

Media type name: audio

Media subtype name: scip

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Binary. This media subtype is only defined for transfer via RTP. There SHALL be no encoding/decoding (transcoding) of the audio stream as it traverses the network.

Security considerations: See Section 7.

Interoperability considerations: N/A

Published specifications: [SCIP210]

Applications which use this media: N/A

Fragment Identifier considerations: none

Restrictions on usage: N/A

Additional information:

1. Deprecated alias names for this type: N/A
2. Magic number(s): N/A
3. File extension(s): N/A
4. Macintosh file type code: N/A
5. Object Identifiers: N/A

Person to contact for further information:

1. Name: Michael Faller and Daniel Hanson
2. Email: michael.faller@gd-ms.com and dan.hanson@gd-ms.com

Intended usage: Common

Authors:

Michael Faller - michael.faller@gd-ms.com

Daniel Hanson - dan.hanson@gd-ms.com

Change controller:

SCIP Working Group - ncia.cis3@ncia.nato.int

5.2. Media Subtype "video/scip"

Media type name: video

Media subtype name: scip

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Binary. This media subtype is only defined for transfer via RTP. There SHALL be no encoding/decoding (transcoding) of the video stream as it traverses the network.

Security considerations: See Section 7.

Interoperability considerations: N/A

Published specifications: [SCIP210]

Applications which use this media: N/A

Fragment Identifier considerations: none

Restrictions on usage: N/A

Additional information:

1. Deprecated alias names for this type: N/A

2. Magic number(s): N/A

3. File extension(s): N/A

4. Macintosh file type code: N/A

5. Object Identifiers: N/A

Person to contact for further information:

1. Name: Michael Faller and Daniel Hanson

2. Email: michael.faller@gd-ms.com and dan.hanson@gd-ms.com

Intended usage: Common

Authors:

Michael Faller - michael.faller@gd-ms.com

Daniel Hanson - dan.hanson@gd-ms.com

Change controller:

SCIP Working Group - ncia.cis3@ncia.nato.int

5.3. Mapping to SDP

The mapping of the above defined payload format media subtype and its parameters SHALL be implemented according to Section 3 of [RFC4855].

Since SCIP includes its own facilities for capabilities exchange, it is only necessary to negotiate the use of SCIP within SDP Offer/ Answer; the specific codecs to be encapsulated within SCIP are then negotiated via the exchange of SCIP control messages.

The information carried in the media type specification has a specific mapping to fields in the Session Description Protocol (SDP) [RFC8866], which is commonly used to describe RTP sessions. When SDP is used to specify sessions employing the SCIP codec, the mapping is as follows:

- The media type ("audio") goes in SDP "m=" as the media name for audio/scip, and the media type ("video") goes in SDP "m=" as the media name for video/scip.

- The media subtype ("scip") goes in SDP "a=rtpmap" as the encoding name. The required parameter "rate" also goes in "a=rtpmap" as the clock rate.

- The optional parameters "ptime" and "maxptime" go in the SDP "a=ptime" and "a=maxptime" attributes, respectively.

An example mapping for audio/scip is:

```
m=audio 50000 RTP/AVP 96
a=rtpmap:96 scip/8000
```

An example mapping for video/scip is:

```
m=video 50002 RTP/AVP 97
a=rtpmap:97 scip/90000
```

An example mapping for both audio/scip and video/scip is:

```
m=audio 50000 RTP/AVP 96
a=rtpmap:96 scip/8000
m=video 50002 RTP/AVP 97
a=rtpmap:97 scip/90000
```

5.4. SDP Offer/Answer Considerations

In accordance with the SDP Offer/Answer model [RFC3264], the SCIP device SHALL list the SCIP payload type number in order of preference in the "m" media line.

For example, an SDP Offer with scip as the preferred audio media subtype:

```
m=audio 50000 RTP/AVP 96 0 8
a=rtpmap:96 scip/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
```

6. Security Considerations

RTP packets using the payload format defined in this specification are subject to the security considerations discussed in the RTP specification [RFC3550], and in any applicable RTP profile such as RTP/AVP [RFC3551], RTP/AVPF [RFC4585], RTP/SAVP [RFC3711], or RTP/SAVPF [RFC5124]. However, as "Securing the RTP Protocol Framework: Why RTP Does Not Mandate a Single Media Security Solution" [RFC7202] discusses, it is not an RTP payload format's responsibility to discuss or mandate what solutions are used to meet the basic security goals like confidentiality, integrity, and source authenticity for RTP in general. This responsibility lies on anyone using RTP in an application. They can find guidance on available security mechanisms and important considerations in "Options for Securing RTP Sessions" [RFC7201]. Applications SHOULD use one or more appropriate strong security mechanisms. The rest of this Security Considerations section discusses the security impacting properties of the payload format itself.

This RTP payload format and its media decoder do not exhibit any significant non-uniformity in the receiver-side computational complexity for packet processing, and thus do not inherently pose a denial-of-service threat due to the receipt of pathological data. Nor does the RTP payload format contain any active content.

SCIP only encrypts the contents transported in the RTP payload; it does not protect the RTP header or RTCP packets. Applications requiring additional RTP header and/or RTCP security might consider mechanisms such as SRTP [RFC3711], however these additional mechanisms are considered OPTIONAL in this document.

7. IANA Considerations

The audio/scip and video/scip media subtypes have previously been registered with IANA [AUDIOSCIP] [VIDEOSCIP]. IANA should update [AUDIOSCIP] and [VIDEOSCIP] to reference this document upon publication.

8. SCIP Contact Information

The SCIP protocol is maintained by the SCIP Working Group. The current SCIP-210 specification may be requested from the email address below.

SCIP Working Group, CIS3 Partnership
NATO Communications and Information Agency
Oude Waalsdorperweg 61
2597 AK The Hague, Netherlands
Email: ncia.cis3@ncia.nato.int

An older public version of the SCIP-210 specification can be downloaded from https://www.iad.gov/SecurePhone/index.cfm.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2736] Handley, M. and C. Perkins, "Guidelines for Writers of RTP Payload Format Specifications", BCP 36, RFC 2736, DOI 10.17487/RFC2736, December 1999, <https://www.rfc-editor.org/info/rfc2736>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, DOI 10.17487/RFC3264, June 2002, <https://www.rfc-editor.org/info/rfc3264>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, DOI 10.17487/RFC3551, July 2003, <https://www.rfc-editor.org/info/rfc3551>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <https://www.rfc-editor.org/info/rfc3711>.

[RFC4585] 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, DOI 10.17487/RFC4585, July 2006, <https://www.rfc-editor.org/info/rfc4585>.

[RFC5124] Ott, J. and E. Carrara, "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)", RFC 5124, DOI 10.17487/RFC5124, February 2008, <https://www.rfc-editor.org/info/rfc5124>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8866] Begen, A., Kyzivat, P., Perkins, C., and M. Handley, "SDP: Session Description Protocol", RFC 8866, DOI 10.17487/RFC8866, January 2021, <https://www.rfc-editor.org/info/rfc8866>.

9.2. Informative References

[AUDIOSCIP] Faller, M. and D. Hanson, "audio/scip: Internet Assigned Numbers Authority (IANA)", 28 January 2021, <https://www.iana.org/assignments/media-types/audio/scip>.

[RFC4040] Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call", RFC 4040, DOI 10.17487/RFC4040, April 2005, <https://www.rfc-editor.org/info/rfc4040>.

[RFC4855] Casner, S., "Media Type Registration of RTP Payload Formats", RFC 4855, DOI 10.17487/RFC4855, February 2007, <https://www.rfc-editor.org/info/rfc4855>.

[RFC4961] Wing, D., "Symmetric RTP / RTP Control Protocol (RTCP)", BCP 131, RFC 4961, DOI 10.17487/RFC4961, July 2007, <https://www.rfc-editor.org/info/rfc4961>.

[RFC5109] Li, A., Ed., "RTP Payload Format for Generic Forward Error Correction", RFC 5109, DOI 10.17487/RFC5109, December 2007, <https://www.rfc-editor.org/info/rfc5109>.

[RFC5761] Perkins, C. and M. Westerlund, "Multiplexing RTP Data and Control Packets on a Single Port", RFC 5761, DOI 10.17487/RFC5761, April 2010, <https://www.rfc-editor.org/info/rfc5761>.

[RFC6184] Wang, Y.-K., Even, R., Kristensen, T., and R. Jesup, "RTP Payload Format for H.264 Video", RFC 6184, DOI 10.17487/

RFC6184, May 2011, <https://www.rfc-editor.org/info/rfc6184>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

[RFC7201] Westerlund, M. and C. Perkins, "Options for Securing RTP Sessions", RFC 7201, DOI 10.17487/RFC7201, April 2014, <https://www.rfc-editor.org/info/rfc7201>.

[RFC7202] Perkins, C. and M. Westerlund, "Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security Solution", RFC 7202, DOI 10.17487/RFC7202, April 2014, <https://www.rfc-editor.org/info/rfc7202>.

[RFC8083] Perkins, C. and V. Singh, "Multimedia Congestion Control: Circuit Breakers for Unicast RTP Sessions", RFC 8083, DOI 10.17487/RFC8083, March 2017, <https://www.rfc-editor.org/info/rfc8083>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <https://www.rfc-editor.org/info/rfc8085>.

[RFC8088] Westerlund, M., "How to Write an RTP Payload Format", RFC 8088, DOI 10.17487/RFC8088, May 2017, <https://www.rfc-editor.org/info/rfc8088>.

[RFC8130] Demjanenko, V. and D. Satterlee, "RTP Payload Format for the Mixed Excitation Linear Prediction Enhanced (MELPe) Codec", RFC 8130, DOI 10.17487/RFC8130, March 2017, <https://www.rfc-editor.org/info/rfc8130>.

[RFC9143] Holmberg, C., Alvestrand, H., and C. Jennings, "Negotiating Media Multiplexing Using the Session Description Protocol (SDP)", RFC 9143, DOI 10.17487/RFC9143, February 2022, <https://www.rfc-editor.org/info/rfc9143>.

[RFC9170] Thomson, M. and T. Pauly, "Long-Term Viability of Protocol Extension Mechanisms", RFC 9170, DOI 10.17487/RFC9170, December 2021, <https://www.rfc-editor.org/info/rfc9170>.

[RMCAT] IETF, "RTP Media Congestion Avoidance Techniques (rmcat) Working Group", <https://datatracker.ietf.org/wg/rmcat/about/>.

[SCIP210]
SCIP Working Group, "SCIP Signaling Plan", SCIP-210, r3.11, September 2023, <https://www.iad.gov/SecurePhone/index.cfm>.

[VIDEOSCIP] Faller, M. and D. Hanson, "video/scip: Internet Assigned Numbers Authority (IANA)", 28 January 2021, <https://www.iana.org/assignments/media-types/video/scip>.

Authors' Addresses

Daniel Hanson
General Dynamics Mission Systems, Inc.
150 Rustcraft Road
Dedham, MA 02026
United States of America

Email: dan.hanson@gd-ms.com

Michael Faller
General Dynamics Mission Systems, Inc.
150 Rustcraft Road
Dedham, MA 02026
United States of America

Email: michael.faller@gd-ms.com

Keith Maver
General Dynamics Mission Systems, Inc.
150 Rustcraft Road
Dedham, MA 02026
United States of America

Email: keith.maver@gd-ms.com