AVTCORE WG
IETF 113

Hybrid Meeting
Friday, March 25, 2022
09:00 - 11:00 UTC
05:00 - 07:00 US/Eastern Time

Mailing list: avtcore@ietf.org
Jabber Room: avtcore@jabber.ietf.org
MeetEcho link: https://wws.conf.meetecho.com/conference/?group=avtcore

This session is being recorded

IETF 113 Meeting Tips

- **Everyone**
  - IETF 113 registration and a datatracker login required to attend
  - Please state your full name before speaking.
  - Join the session Jabber room via IETF Datatracker Meeting Agenda.
- **In person participants**
  - Please sign the (virtual) bluesheets by logging into Meetecho
  - **<u>If you want to join the mic queue, you MUST join the session via Meetecho using either the "onsite" version or regular "remote" version</u>**
  - *Keep audio and video off if not using the onsite version*
- **Remote participants**
  - Make sure your audio and video are off unless you are chairing or presenting during a session or it's your turn in the queue
  - Use of a headset is strongly recommended
  - No need to fill in bluesheets, it’s automatic

This session is being recorded

IETF 113 Remote Meeting Tips

- Enter the queue with  , leave with 
- When you are called on, you need to enable your audio to be heard.
- Audio is enabled by unmuting  and disabled by muting 
- Video can also be enabled, but it is separate from audio.
- Video is encouraged to help comprehension but not required.

Resources for IETF 113 Vienna

- General information:
  https://www.ietf.org/how/meetings/113
- Agenda:
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/113/preparation
- For technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Note really well

- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need to confidentially raise concerns about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior -- in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

About this meeting

- Agenda: https://datatracker.ietf.org/doc/agenda-113-avtcore/
- Notes: https://notes.ietf.org/notes-ietf-113-avtcore
- Jabber Room: avtcore@jabber.ietf.org
- Secretariat: mtd@jabber.ietf.org
- WG Chairs: Jonathan Lennox & Bernard Aboba
- Jabber Scribe:
- Note takers:

Agenda

1. Note Well, Note Takers, Agenda Bashing, Draft status, Liaisons (Chairs, 15 min)
2. Cryptex (S. Murillo & R. Barnes, 15 min)
   https://datatracker.ietf.org/doc/html/draft-ietf-avtcore-cryptex
   https://github.com/juberti/cryptex/issues
3. SCIP (Daniel Hanson, 15 minutes)
   https://datatracker.ietf.org/doc/html/draft-ietf-avtcore-rtp-scip
4. RFC7983bis (B. Aboba, 15 min)
   https://datatracker.ietf.org/doc/html/draft-ietf-avtcore-rfc7983bis
5. SDP for RTP over QUIC (S. Dawkins, 15 min)
   https://datatracker.ietf.org/doc/html/draft-dawkins-sdp-rtp-quic
6. Game Moves over RTP (C. Jennings, 15 min)
   https://datatracker.ietf.org/doc/html/draft-jennings-dispatch-game-state-over-rtp
7. Wrapup and Next Steps (Chairs, 15 min)

Document Status

- Published
  - RFC 8888: was draft-ietf-avtcore-cc-feedback-message
  - RFC 9071: was draft-ietf-avtcore-multi-party-rtt-mix
  - RFC 9134: was draft-ietf-payload-rtp-jpegxs

Document Status (2)

- RFC Editor Queue
  - draft-ietf-payload-vp9 (MISSREF)
- In IETF Last Call (ends April 5, 2022)
  - draft-ietf-avtcore-cryptex
- Publication Requested
  - draft-ietf-avtext-framemarking
- Awaiting Chair Writeup
  - draft-ietf-avtcore-rtp-vvc
- Adopted
  - draft-ietf-avtcore-rtp-scip
  - draft-ietf-avtcore-rtp-evc
  - draft-ietf-avtcore-rfc7983bis

VVC RTP Payload Format IPR

- Two IPR declarations have been submitted relating to draft-ietf-avtcore-rtp-vvc:
  - Declaration 4048, received on March 10, 2020: Tencent Technology (Shenzhen) Company Limited's Statement about IPR related to draft-ietf-avtcore-rtp-vvc
  - Declaration 4914, received on June 13, 2021: Nokia Technologies Oy's Statement about IPR related to draft-ietf-avtcore-rtp-vvc
- An IPR notice was sent to the WG on March 8, 2022: https://mailarchive.ietf.org/arch/msg/avt/vH-1ZgsF0EMBqIUy64apLQqLI78/
- Are there objections to proceeding with this document?

Recent Liaison Statements

- Request from W3C WebTransport WG
  - Presented at IETF 112.
  - Proposed response is here.
- Liaison from ISO/IEC JTC 1/SC 29/WG 03
  - Subject: MPEG Green Metadata
  - Received: October 22, 2021
  - Link is here.
  - Response (sent) is here.

W3C WebTransport Request

- The W3C WebTransport WG has identified problems with bidirectional realtime audio/video communication over WebTransport, particularly: a client sending media to the server:
  - **Problem:** The client doesn't have enough information to know when it can reapply a multiplicative increase in the media send rate to recover from prior congestion.
  - **Requests**:
    i. To know if RTP over QUIC can satisfy this use case.
    ii. If so, what measurements can a browser make available to a JS client, to assist with this problem.
    iii. Will selectable congestion control be required? And if so, which algorithm(s)?

Proposed Response

https://mailarchive.ietf.org/arch/msg/avt/QyOqHcsCHCi_ayV73IDChKGOR9k/

[AVTCORE] Response to W3C WebTransport WG Request from IETF 112

Bernard Aboba <bernard.aboba@gmail.com> | Wed, 16 February 2022 01:13 UTC | Show header

At IETF 112, the W3C WebTransport WG presented a request for feedback to the AVTCORE WG:
https://docs.google.com/presentation/d/1XB-RTt-ejDTillmkYcT3l6EBzNK7pARw51TqKcCxo8A/edit#slide=id.gfc2dae0c1a_0_125

The request related to problems encountered with W3C WebTransport API use cases involving attempts to send media with low latency from client -> server. Currently, WebTransport implementations are based on BBRv1 congestion control in QUIC and support datagram prioritization in an effort to improve QUIC datagram latency.

The presentation today from M. Engelbart appears to shed light on the request, even though the results presented were based on NewReno CC instead of BBRv2/v2.

Based on the experimental results, can we make any recommendations? For example, can we say:

1. Attempting to implement a low-latency congestion control algorithm for QUIC datagrams (e.g. SCReaM or GCC) on top of QUIC congestion control (New Reno, BBRv1/v2) isn't recommended. Instead, it is preferred to implement an alternative CC algorithm within the QUIC implementation.

2. Naive prioritization schemes such as strict priority for QUIC datagrams result in high queueing delays, since reliable stream data will fill the congestion window when datagrams aren't being sent. This problem will occur even with CC algorithms such as BBRv1/v2 (not just NewReno).

Completely Encrypting RTP Header Extensions and Contributing Sources (Cryptex)

https://datatracker.ietf.org/doc/html/draft-ietf-avtcore-cryptex

https://github.com/juberti/cryptex/issues

Sergio Garcia Murillo and Richard Barnes

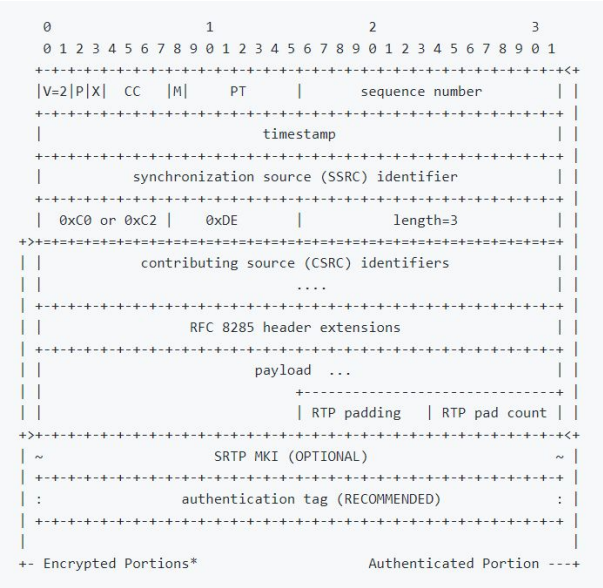
Current Status

- In IETF Last Call (ends April 5, 2022)
  - [AVTCORE] Last Call: <draft-ietf-avtcore-cryptex-05.txt> (Completely Encrypting RTP Header Extensions and Contributing Sources) to Proposed Standard
  - Contact name & email address for IANA registration (Issue 43) to be handled after IETF last call.
  - Directorate reviews (including SDP review) to follow.

Issue 31: Encryption processing is under-specified

- PR for adding clarifications to the plaintext and associated data available
  - https://github.com/juberti/cryptex/pull/45

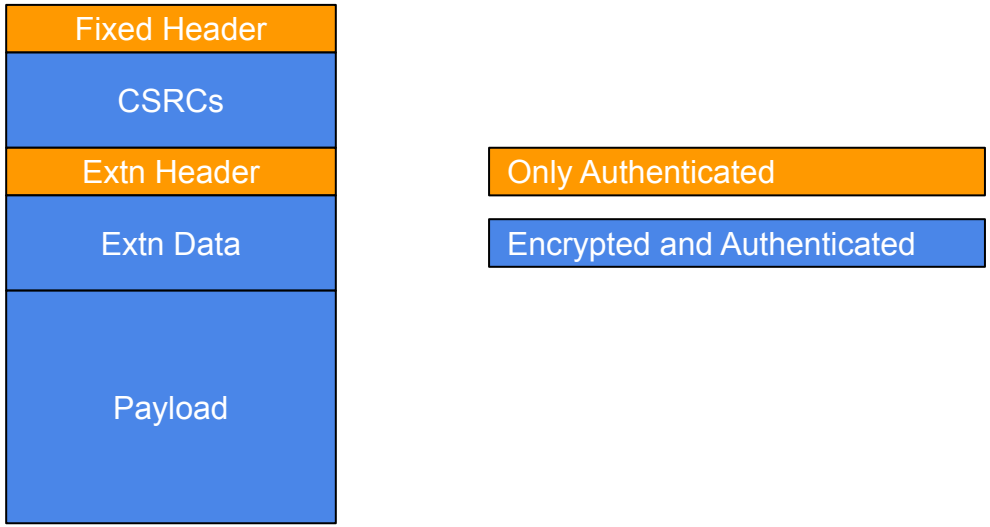
```
Plaintext = CSRC identifiers (if used) || header extension ||
     RTP payload || RTP padding (if used) || RTP pad count (if used).

Associated Data: The version V || padding flag P || extension flag X ||
     Contributing Source (CSRC) count CC || marker M ||
     Payload Type PT (7 bits) || sequence number  || timestamp || SSRC ||
     extension header ("defined by profile" || extension header length).
```



Recall: Cryptex encryption

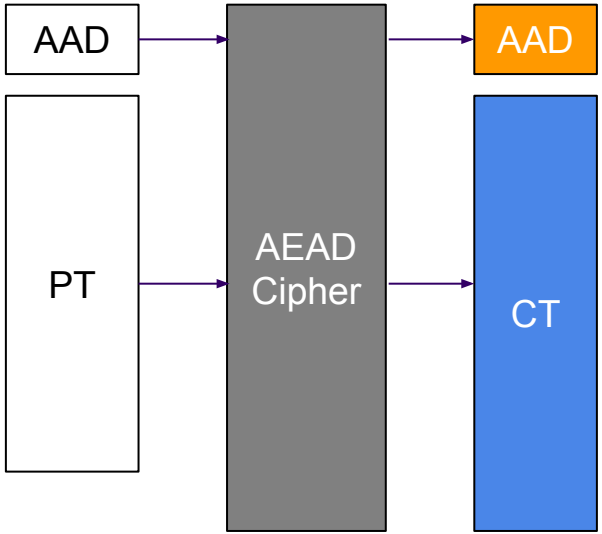
Goal: Encrypt CSRCs, Extension data, and Payload in one operation

“Punctured” to not encrypt extension header, so that packets parse normally

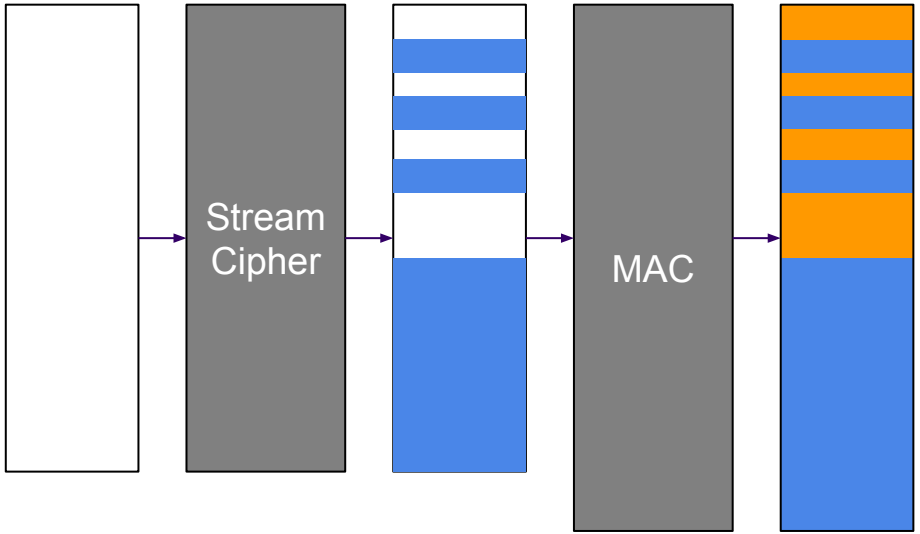


Recall: Encryption Interfaces

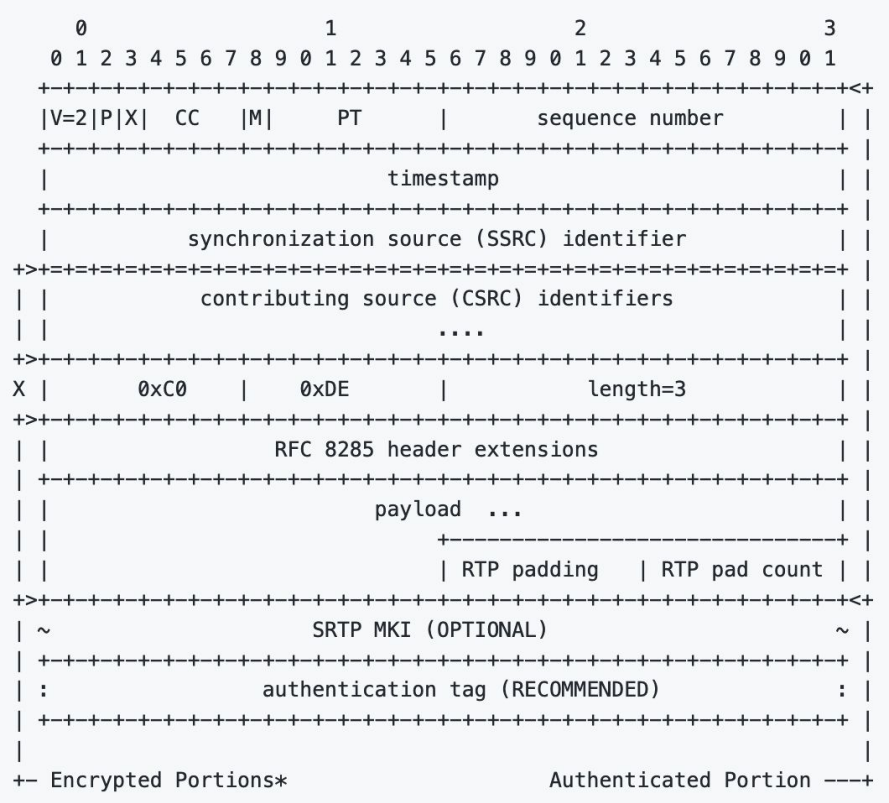
AEAD
(e.g., AES-GCM)



Stream Cipher + MAC
(e.g., AES-CTR + HMAC-SHA256)



Spec today is ambiguous



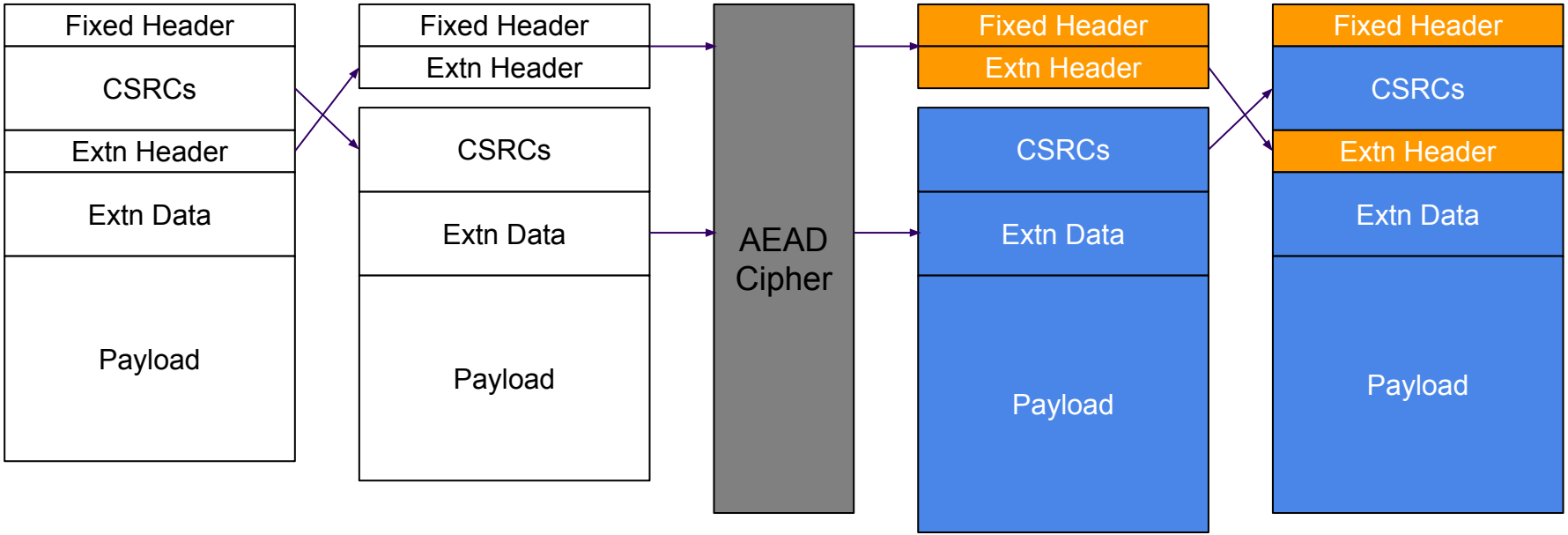
If AEAD: How to construct a contiguous, non-punctured plaintext input?

If stream cipher: What stream cipher is used with AEAD-based protection profiles?

Option 1: AEAD-like

Pro: AEAD is the way of the future

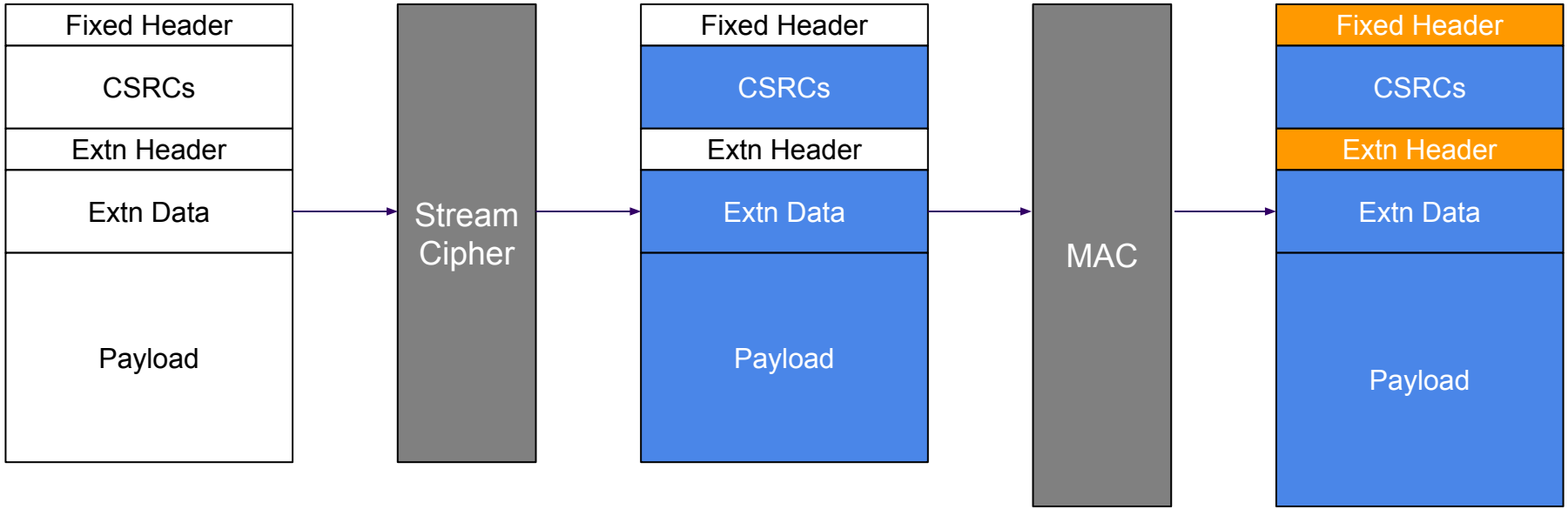
Con: memcpy of 4*CC + 4 bytes



Option 2: Stream-like

Pro: Easy in-place implementation

Con: Locked into stream cipher



Proposal: Option 1 (AEAD)

AEAD is the way of the future

Memcpy is not that expensive

RTP Payload Format for the SCIP Codec

Daniel Hanson

and

Michael Faller

https://datatracker.ietf.org/doc/html/draft-scip-payload-00

SCIP RFC - Background, Issue, and Purpose

- The Secure Communication Interoperability Protocol (SCIP) began in 1994 in the U.S. and includes NATO and NATO partners
  - Devices using the signaling in the SCIP Draft RFC are presently deployed in products used by US and NATO
- Devices that implement the SCIP standards operate over digital carriers and require network devices to transparently support SCIP codecs
- Most commercial network administrators and security personnel are not aware of SCIP
  - Can result in the SCIP media subtype “scip” being removed from the SDP
- SCIP RFC provides a globally accessible reference to increase awareness
- The SCIP RFC was accepted as a AVTCORE work item in January 2022
  - Comments received have been reviewed and incorporated into a new draft SCIP RFC

Overview of SCIP

- Two media subtypes “audio/scip” and “video/scip” have been registered with IANA as RTP Payload Format Media Types
- The SCIP RFC is needed to provide additional information for these media subtypes (RTP Header Fields, Payload Format Parameters)
- 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
```

Call for Adoption - SCIP Draft RFC Comments and Updates (1 of 2)

- Changes due to comments on Section 4.1:
  - Conformance to RFC 3550 changed from “should” to “shall”
  - Added text to stipulate that the network should not repacketize SCIP packets
  - Modified wording related to the use of the marker bit
    - Marker bit shall be set to zero for discontinuous traffic
    - Marker bit for continuous traffic will be based on underlying media subtype specification (unchanged)

Call for Adoption - SCIP Draft RFC Comments and Updates (2 of 2)

- Response to comment on Section 5.1/5.2: Interoperability considerations: N/A
  - "N/A" was specified because there are no previous versions of the SCIP submedia type
- Changes due to comments on Section 8.1/8.2:
  - References to SCIP-214.2 and SCIP-210 moved from normative to informational
- Document name changed to "draft-ietf-avtcore-rtp-scip-00"

Summary, Conclusions, and Questions

- Issues have occurred because OEMs of network equipment, network administrators and security personnel are unaware of SCIP and SDP contents necessary to establish a secure session
- The purpose of the SCIP RFC is to provide global access to information necessary to support SCIP
  - Provides information to Network Equipment OEMs and Network Operators/SysAdmins
- Comments received during the AVTCORE Call for Adoption period have been reviewed and incorporated into the draft RFC
  - Since then, no new comments have been received
- Questions?
- What is the next step?

RFC 7983bis

Bernard Aboba

G. Salgueiro

C. Perkins

https://datatracker.ietf.org/doc/html/draft-ietf-avtcore-rfc7983bis

RFC 7983bis

- Update to RFC 7983 Section 7, documenting QUIC multiplexing.
  - Description of multiplexing SRTP, SRTCP, STUN, TURN, DTLS, ZRTP and QUIC
  - Guidance on handling overlap between QUIC and TURN channels (not an issue in WebRTC).
- Update to (D)TLS Content-Type Field IANA page to reference new RFC (no other change needed)
- Caveat:
  - “Since new versions of QUIC are allowed to change aspects of the wire image, there is no guarantee that future versions of QUIC beyond version 1 will adhere to the multiplexing scheme described in this document.”

RFC 7983bis-02

- Changes from -01:
  - Clarification of multiplexing scenarios:
    - SRTP/SRTCP for media, DTLS-SRTP key management, QUIC for data exchange
      - Does not require replacement of QUIC congestion control algorithms.
    - RTP over QUIC
      - Requires multiplexing of QUIC with STUN/TURN.
  - Reference updates:
    - RFC 8489 (STUN)
    - RFC 8656 (TURN)
    - RFC 9000 (QUIC transport)
    - RFC 9001 (QUIC-TLS)
  - All normative references now published as RFCs.
- Next steps: Ready for WGLC?

SDP for RTP over QUIC

(Sooo many Issues!)

Spencer Dawkins

~~https://datatracker.ietf.org/doc/html/draft-dawkins-sdp-rtp-quic~~

https://github.com/SpencerDawkins/sdp-rtp-quic-issues

The Education of Spencer

- What I THOUGHT I was doing in draft-dawkins-avtcore-sdp-rtp-quic-00
  - “What SDP do you need to do a drop-in replacement for SRTP?”
- What I was ACTUALLY doing
  - Trying to keep track of questions for “RTP over QUIC”
  - (because many of these questions might impact SDP)
  - (in at least three different places, because of various reasons)
- What I THINK I’m going to do, between now and IETF 114
  - Hold off on updating draft-dawkins-avtcore-sdp-rtp-quic-00 for now
  - Collect the questions from various locations as GitHub Issues
  - THEN start working on answers, and updating the SDP draft

Caveat Lector

- Some of these issues may be tied to non-traditional RTP use cases
  - Insert WebRTC by reference here
  - Insert Media Over QUIC BOF by reference here
- I'm tracking these issues anyway
  - Possible for RTP to use QUIC like other Media Transport Protocols do

Issues from the interim (transferred)

- Does double encryption matter for (say) SAVPF? #5
- Will we need a QUIC adaptation layer for RTP/RTCP #4
- Distinguishing between mappings onto streams and onto datagrams? #3
- Feedback from RTCP, QUIC, some of each, or something else?? #2
- *Check QUIC impacts on BUNDLE* #5
- *Consider including a=tls-id in SDP* #6
- *Consider including a=fingerprint mechanism in a p2p SDP example* #7
- Signaling media-friendly congestion control? #1

New and exciting issues from Bernard

- QUIC for data exchange? #9
- RTP over reliable streams or datagrams? #8
- Exchange of Fingerprints #7
- RTP over QUIC topologies #6

Issues in the TEXT of the SDP draft 👀

- Decouple the RTP state machine and the QUIC state machine #11
- QUIC connection migration in case of path failure #10

Issues I’d like feedback on

- Does double encryption matter for (say) SAVPF? #5
- Distinguishing between mappings onto streams and onto datagrams? #3
- QUIC connection migration in case of path failure #10

Does double encryption matter? #5

- Initial draft - define "QUIC/RTP/SAVP" and "QUIC/RTP/SAVPF"
  - Great plan! Ignore SAVP/SAVPF over QUIC
  - QUIC encrypts more than SRTP anyway
  - BUT use that as a hint(?) to forward over unencrypted protocols
- Comment - this is silly. Define AVPF and tell the truth
  - QUIC encrypts more than SRTP anyway
  - Use explicit signaling to tell RTP middleboxes how to forward
  - Implemented this as PR #9
- Comment - Not so fast! What about apps that use SAVP/SAVPF?

So - what happens next

- What I THINK I'm going to do, between now and IETF 114
  - Hold off on updating draft-dawkins-avtcore-sdp-rtp-quic-00 for now
  - Collect the questions from various locations as GitHub Issues
  - THEN start working on answers, and updating the SDP draft
- I appreciate feedback, and I appreciate proposed text as well
  - That can happen on the AVTCORE mailing list, or in GitHub
- No need to request adoption of anything at this time
  - AVTCORE doesn't have an adopted RTP over QUIC draft yet
  - If SDP draft is adopted, AVTCORE chairs request MMUSIC review

So, any questions or comments?

Game Moves Over RTP

Cullen Jennings

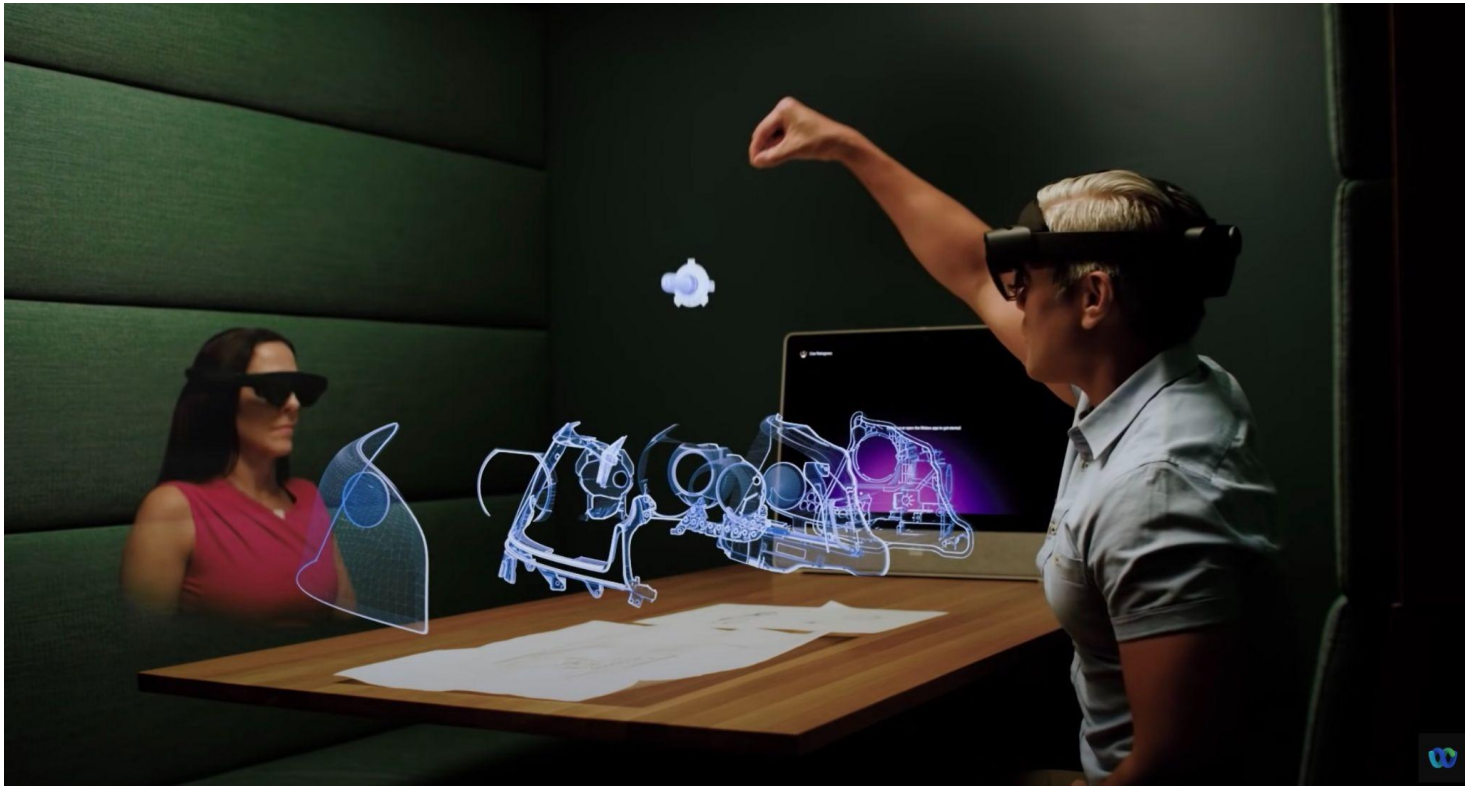
Rich Logan

https://datatracker.ietf.org/doc/html/draft-jennings-dispatch-game-state-over-rtp

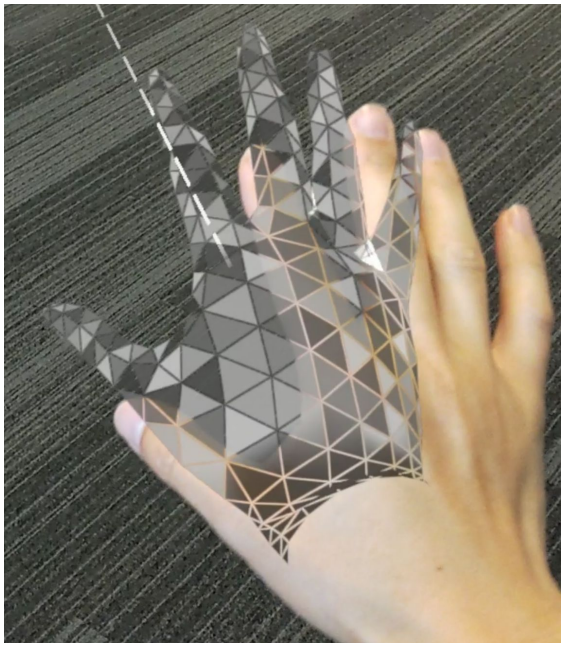
Goals

- Online real time gaming needs to synchronize player and game object state
  - Many proprietary solutions: Unity UTP, Nvidia Omniverse.
- Low latency is critical.
- Large scale is critical.
- Bandwidth efficiency is important.
- Often need synchronization with other media
- Easily extensible as many applications have their own data needs

Example



Example Data



Microsoft Mixed Reality Toolkit (MRTK) widely used

- Encode hand joint locations in RTP
- Encode rate of change
- Allows receiver to render smooth hand motion

Solution

- Use RTP
  - lots of things don’t want RTP but lots do
- Support for current state and rate of change
- Extensible structured data with TLVs (tag, length, value)
- Binary based encoding with defined structures
- Extensible Framework for any application
- Applications can easily get a code point for their schema

Status

Current draft is enough to see the design and flavor of the solution

Draft needs:

- lots more RTP crank wheel template stuff
- broader input of base types and objects

Open source implementation: https://github.com/cisco/gse

Ask

We are trying to make interoperability between 3D meetings, metaverse systems, and real time gaming

- Need to be able to move forward relatively quickly, if IETF is the wrong place to do this let us know now
  - Is this in scope for AVTCore ?
  - Could we move forward with base draft and non controversial objects (move controversial object to extension drafts)
- What other objects do people have a use case for that should be added ?

Wrapup and Next Steps

- Action items
- Next steps

Thank you

Special thanks to:

The Secretariat, WG Participants & ADs