sframe

IETF 109, Somewhere Thailand Somewhere

caveat participem

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)

agenda

welcome, administrivia, agenda	5 chairs
charter review	10 chairs
Use Cases - Conferencing	10 Emad Omara
- Streaming	10 Dr. Alex Gouaillard
- WebRTC	10 Youenn Fablet
Protection	30 Emad Omara
Protection for - Video Payloads	20 Sergio Garcia Murillo
MLS Integration	20 Richard Barnes

Charter Overview

Primary Goal -

- End-to-end encryption for real-time conferencing sessions
- Separated from the transport layer
- Exposed (but authenticated) media metadata useful for Selective Forwarding Units (SFUs, *aka* RTP Switches)

"This working group will define the SFrame secure encapsulation to provide authenticated encryption for real-time media content that is independent of the underlying transport..." (*https://datatracker.ietf.org/wg/sframe/charter/*)

Charter Goals and Non-Goals

Out of scope:

- Signalling required to arrange SFrame encryption
- Especially - Considerations related to SIP or SDP
  - Motivation: SFrame is intended to be applied as an additional layer on top of the base levels of protection that these protocols provide
- Other WebRTC changes such as the payload format and metadata format
  - Motivation: will be addressed by the AVTCORE working group

Charter Goals and Non-Goals (cont'd)

In scope:

- Define guidance for how SFrame interacts with RTP
- Especially with regard to *packetization*, *depacketization*, and *recovery* algorithms
  - Motivation: to ensure that it can be used in environments such as WebRTC

- Security properties and implications under common threat models

Charter Goals and Non-Goals (cont'd)

In scope (cont'd):

- Mechanism for doing SFrame encryption using keys from MLS
  - Motivation: It is anticipated that several use cases of SFrame will involve its use with keys derived from the MLS group key exchange protocol
  - Does not preclude other sources of key material

Charter Overview: Encapsulation

- Transport Independent - SFrame secure encapsulation is transport-independent
  - It can be applied at a higher level than individual RTP payloads
- Multi-packet Frames - E.g., encrypting entire frames that span multiple packets: amortizing framing and authentication tag overhead
- Intermediate Sized Units - Or encrypting units of intermediate size (H.264 NALUs or AV1 OBUs) to allow partial frames to be usable
- Granularity Levels TBD - WG to choose what levels of granularity can be selected in the protocol

Charter Overview: Encapsulation (cont'd)

The encapsulation provides the following for authenticated encryption for each encryption operation:

- Selection among multiple encryption keys in use during a real-time session
- An algorithm for forming a unique nonce within the scope of the key based on information in the encapsulation framing

Charter Overview: Encapsulation (cont'd)

An application using SFrame will need to choose several aspects of its operation, for example:

- Selecting whether SFrame is to be used for a given media flow
- Specifying which encryption algorithm should be used
- Provisioning keys and key identifiers to endpoints
- Selecting the granularity at which SFrame encryption is applied (if multiple options are available)

agenda

welcome, administrivia, agenda	5 chairs
charter review	10 chairs
Use Cases - Conferencing	10 Emad Omara
- Streaming	10 Dr. Alex Gouaillard
- WebRTC	10 Youenn Fablet
Protection	30 Emad Omara
Protection for - Video Payloads	20 Sergio Garcia Murillo
MLS Integration	20 Richard Barnes

our charter

Real-time conferencing sessions increasingly require end-to-end protections that prevent intermediary servers from decrypting real-time media. The PERC WG developed a “double encryption” scheme for end-to-end encryption that was deeply tied to SRTP as its underlying transport. This entanglement has prevented widespread deployment.

our charter (cont'd)

This working group will define the SFrame secure encapsulation to provide authenticated encryption for real-time media content that is independent of the underlying transport. The encapsulation will provide the following information to drive the authenticated encryption for each encryption operation:

- Selection among multiple encryption keys in use during a real-time session
- An algorithm for forming a unique nonce within the scope of the key based on information in the encapsulation framing

our charter (cont'd)

The SFrame specification will detail the specific security properties that the encapsulation provides, and discuss their implications under common usage scenarios / threat models.

our charter (cont'd)

The transport-independence of this encapsulation means that it can be applied at a higher level than individual RTP payloads. For example, it may be desirable to encrypt whole frames that span multiple packets in order to amortize the overhead from framing and authentication tags. It may also be desirable to encrypt units of intermediate size (e.g., H.264 NALUs or AV1 OBUs) to allow partial frames to be usable. The working group will choose what levels of granularity can be selected in the protocol.

our charter (cont'd)

An application using SFrame will need to choose several aspects of its operation, for example:

- Selecting whether SFrame is to be used for a given media flow
- Specifying which encryption algorithm should be used
- Provisioning keys and key identifiers to endpoints
- Selecting the granularity at which SFrame encryption is applied (if multiple options are available)

our charter (cont'd)

This working group, however, will not specify the signaling required to arrange SFrame encryption. In particular, considerations related to SIP or SDP are out of scope. This is because SFrame is intended to be applied as an additional layer on top of the base levels of protection that these protocols provide. This working group will, however, define the guidance for how SFrame interacts with RTP (e.g., with regard to packetization, depacketization, and recovery algorithms) to ensure that it can be used in environments such as WebRTC. Other WebRTC changes such as the payload format and metadata format will be addressed by the AVTCORE working group.

our charter (cont'd)

It is anticipated that several use cases of SFrame will involve its use with keys derived from the MLS group key exchange protocol. The working group will define a mechanism for doing SFrame encryption using keys from MLS, including, for example, the derivation of SFrame keys per MLS epoch and per sender. The availability of this mechanism for using keys from MLS does not preclude the use of other sources of key material.

Jun 2021 - Submit SFrame specification to IESG (Standards Track)