draft-hutton-mmusic-opportunistic-negotiation-00

B. Aboba
A. Hutton
R. Jesske
A. Johnston
G. Salgueiro

Background

- In theory SDP allows different RTP profiles such as SAVP, AVPF, and AVP to be offered as separate m-lines, and allows the answerer to reject profiles it does not support or does not wish to use.
- However using multiple m-lines in this way is not well defined, complex, and fails in the real world.
- Opportunistic approaches to SRTP using a single m-line have been around for over a decade and are widely implemented.
  - draft-kaplan-mmusic-best-effort-srtp-00
  - IMTC SIP Security Best Practice.
- SIP Forum – SIP Trunking specification (SIPconnect2.0) did not include opportunistic security due to lack of RFC.

SIPBrandy Working Group

- Charter States:

  "The working group will additionally coordinate with the MMUSIC working group to define opportunistic security [RFC 7435] for SIP-signaled media sessions for situations where strong protections are not necessary or not feasible".

- Also

  "The working group is not expected to define new protocols or modify existing ones; rather it will define practices for using existing protocols. If the working group discovers gaps that require creation or modification protocols, it will forward those gaps to the appropriate working groups."

- Which is why we are here today:

Opportunistic Security.

- “Some Protection Most of the Time”
- Opportunistic Security is an approach to Security that:
  - Defines a third mode of security between “cleartext” and “comprehensive protection”.
  - Allows encryption and authentication to be used if supported but will not result in failure if not supported.
  - Is not a substitute for authenticated, encrypted communication policies.
- Defined in RFC 7435.

draft-hutton-mmusic-opportunistic-negotiation

- Avoids multiple m-lines by recognising that existing implementation of SRTP, and RTCP feedback, make use of the relevant SDP attributes to indicate such capabilities.
- Opportunistic SRTP – MUST use the AVP Profile.
  - Update to RFC 4569 which states that *"SRTP security descriptions MUST only be used with the SRTP transport (e.g., "RTP/SAVP" or "RTP/SAVPF")"*
  - Procedures for different keying techniques described in draft-ietf-sipbrandy-osrtp.
- Negotiating RTCP Feedback – MUST use the AVP Profile.
  - MUST use the AVP profile and include the "a=rtcp-fb" SDP attribute.
  - Updates [RFC4585] which requires that the "a=rtcp-fb" attribute is only used with the AVPF profile.

PLEASE MMUSIC ADOPT THIS DRAFT

draft-hutton-mmusic-opportunistic-negotiation