ERICSSON

Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)

IETF#81, Quebec City, Canada

draft-ietf-simple-msrp-sessmatch-13

Christer.Holmberg@ericsson.com
Staffan.Blau@ericsson.com

MAJOR CHANGES FROM -11

- **Session matching modification removed**
  - RFC 4975 session matching procedure used
- **SDP c/m-line used for MSRP TCP connection establishment**
- **“Middlebox” terminology used instead of “ALG”**
  - Middlebox definition added

OTHER CHANGES FROM -11

- a=msrp-cema attribute defined
- sessmatch option-tag removed
- Support of RFC 6135 mandatory
  - Helps to avoid cases where a middlebox needs to enable MSRP B2BUA functionality
- Additional applicability statement text
- Additional security considerations text

CEMA ADVANTAGES

- Works with TLS name based authentication.
- Fewer cases where middlexboxes need to enable MSRP B2BUA functionality.
- Allows end-to-end TLS in the presence of middleboxes
  - Previously a middlebox always had to enable MSRP B2BUA.
  - Meaning middlebox had to read plaintext in all situations

MSRP B2BUA BEHAVIOR NEEDED

- RFC 4975 UA is “active”
  - Establishes MSRP TCP connection (based on SDP a=path)
- RFC 4975 UA uses an MSRP relay
  - Also when the RFC 4975 UA is “passive”, as it cannot be assumed that the SDP c/m-line contains the address of the relay (but rather the address of the UA)
- Needed for backwards compatibility

Opportunity for End-to-End Security

- Both UAs support CEMA
- RFC 4975 UA is "passive" (and does not use an MSRP relay)
  - Previous versions of sessmatch required MSRP B2BUA behavior in this case.
- UA supports CEMA and uses MSRP relay
  - Previous versions of sessmatch required MSRP B2BUA behavior in this case.
- MSRP B2BUA BEHAVIOR **NOT** NEEDED

COMMENTS: Topology hiding

- **Comment:** CEMA does not allow MSRP topology hiding, as the a=path attribute can not be modified (without the modifier acting as a MSRP B2BUA).

- **Reply:** Topology hiding was not possible in pre-CEMA versions of sessmatch either, as the MSRP messages are not modified.

COMMENTS: TLS

- **Comment**: Do we need to mandate usage of TLS when communicating with middleboxes?

- **Proposal**: When CEMA UAs communicate, they MUST use TLS for MSRP.

- When communicating with 4975 UAs, the draft refers to the 4975 procedures:

"NOTE: As defined in RFC 4975, if TLS authentication fails, the user need to be able to decide whether to try to anyway establish an MSRP connection."

COMMENTS: Middlebox MSRP B2BUA decision

- Draft currently says:

> *"In cases where support of the CEMA extension is indicated by at least one MSRP endpoint, the Middlebox can simply modifies the SDP c/m-line address information for the MSRP connection."*

- **Comment**: Middlebox needs to make decision when it receives SDP offer.

COMMENTS: Editorial

- MSRP B2BUA definition
- Note that a FQDN (in a=path and/or SDP c-line) needs a DNS lookup in order to check a=path/c-line match)
- Table that shows when MSRP B2BUA enabling is needed.

PROPOSAL TO THE WG

- 1. ADDRESS COMMENTS
- 2. WGLC

THANK YOU FOR LISTENING!