Security Architecture

The (other) open issues

MTI algorithm for a=fingerprint

Proposal: MUST SHA-256, MAY SHA-1

...for both sending and validation

Revise the SHA-1 policy to MUST NOT later

TURN only (1/2)

Magnus says: “I wonder if there are actually needs to be a consideration on the WebRTC implementation to have a user knob that forces it into TURN only mode, so that one can't use the browser to get the local IP.”

This issue has been extensively litigated across blogs. See bug 959893.

TURN only (2/2)

This reopens an issue we closed a while back.

The concern arises out of two things:

- exposure of addresses for “privacy” VPN users
- exposure of LAN topology

Browsers are unable to properly distinguish between “privacy” VPNs and regular VPNs

Real privacy protection requires considerably more sophistication

Proposal: leave this to the browsers

SDES Residue

Magnus notes some text in the draft that seems to imply use of something other than DTLS-SRTP

Proposal: he is right, just remove anything that might be an SDES holdover

WTF NULL

This also appears to be suspect:

The "security characteristics" MUST indicate the cryptographic algorithms in use (For example: "AES-CBC" or "Null Cipher".) However, if Null ciphers are used, that MUST be presented to the user at the top-level UI.

Proposal: remove this dangerous cruft