

# Real-Time Streaming Protocol

## draft-ietf-mmusic-rfc2326bis-07

Magnus Westerlund

Aravind Narasimhan

Henning Schulzrinne

Robert Lanphier

Anup Rao

# Presentation Outline

- Changes
  - Security framework
  - Use cases
  - Other
- Open Issues
  - Keep-Alive
- Way Forward

# Changes: Security Framework

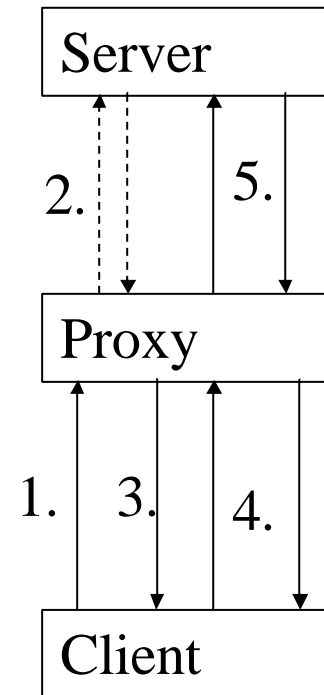
- The security features in RFC 2326 was underspecified, e.g. TLS only hinted.
- To provide defense against hi-jacking attacks encryption of RTSP messages to and from server are need.
- TLS does also provide certain privacy features, like concealing exact content viewed.
- TLS does also prevent ALGs from modifying RTSP messages, which is both good and bad.
- However certain deployment scenarios: company firewalls, private or restricted network, requires proxies, possibly with ALG functionality.

# Changes: Security Framework

- Defined usage of TLS over TCP for RTSP.
- A concept for TLS with trusted proxies as complement to tunnel mode.
  - Client approved
  - Proxy policies
  - Any (for debug)
- Defines the usage of “rtsps”
- Use of HTTP authorization mechanisms clarified.

# TLS connect walkthrough

1. Client connects with TLS and send Request to proxy.
2. Proxy Connects with TLS to server and get certificate.
3. Proxy responds to request with 470, and include server certificate.
4. Client checks certificate and accepts it. Include hash of certificate and resends request.
5. Proxy matches hash with connection and forwards request in TLS.



# RTSP Use Cases

- New chapter that defines the following use cases:
  - On-demand Playback of Stored Content
  - Unicast distribution of Live Content
  - On-demand Playback using Multicast
  - Inviting a RTSP server into a conference
  - Live Content using Multicast
- Only the two first are sufficiently defined to be used in Internet. The rest lacks certain mechanisms or have unsolved security issues.

# Changes: Other 1/2

- Allowing for multiple SSRC values in Transport header.
- ETag & If-None-Match header added and usage clarified.
- OPTIONS has been clarified in regards to Public and Allow header and some of the usage.
- Clarified usage of Public header for proxies.
- Defined the term “RTSP Agent” used in OPTIONS
- Clarified usage of PLAY and ranges, e.g. media packets with long duration.
- Allowed for PLAY request in Playing state, when media has finished, and no support for update has been shown.

# Changes: Other 2/2

- Clarified requirement for sync info in PLAY response.
- REDIRECT clarified.
- Updated boilerplate.
- A number of Editorial changes



# Open Issues 1/4

- Which keep-Alive mechanism to be normative to use?
  - Server SHALL do keep-alive on any method that it gives 1xx, 2xx, or 3xx response to
  - Client is RECOMMENDED to use SET\_PARAMETER for keep-alive.
  - If client receives 501 response to SET\_PARAMETER then OPTIONS needs to be used.
- Should refusal by server to perform media redirection have its own error code?
  - Yes, Sean will write up text proposal for 463.

# Open Issues 2/4

- Change usage of Accept-Language/Content-Language?
  - No, RFC 2326 is clear on this. If desired a separate extension need to be developed.
- Is current methods to prevent undesired media redirection sufficient.
  - Yes, but language will be further sharpened.
- Is the availability of protection against hijacking attacks sufficient?
  - Yes, based on that one can use TLS to protectet Session ID

# Open Issues 3/4

- Should further clarifications on how re-SETUP work be written?
  - No, is to dependent on the combination of transports.
- Lacking Specification text for “Implicit Redirect”?
  - There will at this time be no extension.
  - Clarification that media redirect in session description is not allowed. SETUP after DESCRIBE shall be possible in the same connection.
- How may “#” an “?” in the URI be used?
  - Clarify the standard RFC 2396 rules apply:
    - Fragment “#” is client side and shall not be sent to server
    - Query “?” is server specific

# Open Issue 4/4

- Should further explanation on proxies be written?
  - Yes, but we are missing any volunteer
- Is the changes sufficient backwards compatible, or do we need to raise the version number?
  - Still Inconclusive. However proposal is to continue analysis of the changes performed to determine scope.

# Way Forward 1/2

- Review, Review, and more Review:
  - Is the specification consistent?
  - Is the text understandable?
  - Is something missing?
  - Is something erroneous defined?
  - Is the backwards compatibility seriously affected?

# Way Forward 2/2

- Continue the editing work between meetings.
- Publish a new version when significant changes has been done.
- If needed have phone conferences.
- Aiming at Working Group Last Call after IETF 61.