Connection-Oriented Media Transport over TLS

`draft-ietf-mmusic-comedia-tls-01`

IETF MMusic Working Group
Wednesday, August 4, 2004

Jonathan Lennox
Columbia University
lennox@cs.columbia.edu

Overview

- Want privacy, authentication and integrity for connection-oriented media.
  - Use TLS.
- TLS uses X.509 certificates — must specify what identities certificates should assert.
  - Host-based identity (dNSname or iPAddress), based on host in SDP `c=` line.
  - Certificate which secured the SDP end-to-end (*e.g.* S/MIME or https; not sips).
  - URI-based identity, based on protocol transporting SDP.
- Often, end systems can’t use CA-signed certificates — too expensive, hard to configure, DHCP, etc.
  - Use self-signed certificates; send **certificate fingerprints** (secure hashes of certificates) in SDP.

Example

```
m=image 54111 TCP/TLS t38
c=IN IP4 10.1.1.2
a=setup:passive
a=connid:1
a=fingerprint:MD5 48:AA:D8:BA:36:7C:6D:70:7F:81:BB:BA:ED:6D:B8:C7
```

Open Questions: This Document

- Is this the best way to solve this problem?
- Is it too different from the Security Descriptions draft?
- Is the list of allowed identities correct? Does it need further definition?
  - Should wildcards be allowed in dNSName identities?
  - Does "identity based on protocol transporting SDP" need further definition?
- Is the certificate fingerprint scheme useful? Should it be required for all self-signed certs?
- How strongly should integrity validation for the SDP be required? SHOULD, MUST?

Open Question: Secure Connection-Oriented RTP

- This document defines only `TCP/TLS`, not `TCP/TLS/RTP/AVP`.
- Similarly, nothing defines `TCP/RTP/SAVP`.
- What should be the preferred way of doing secure connection-oriented RTP?
- What draft or drafts should define it?
- (Related problem: combinatorial explosion of `*/RTP/*` proto fields. . .)