University of Glasgow | School of Computing Science

Reflections on Security Options for the Real-time Transport Protocol Framework

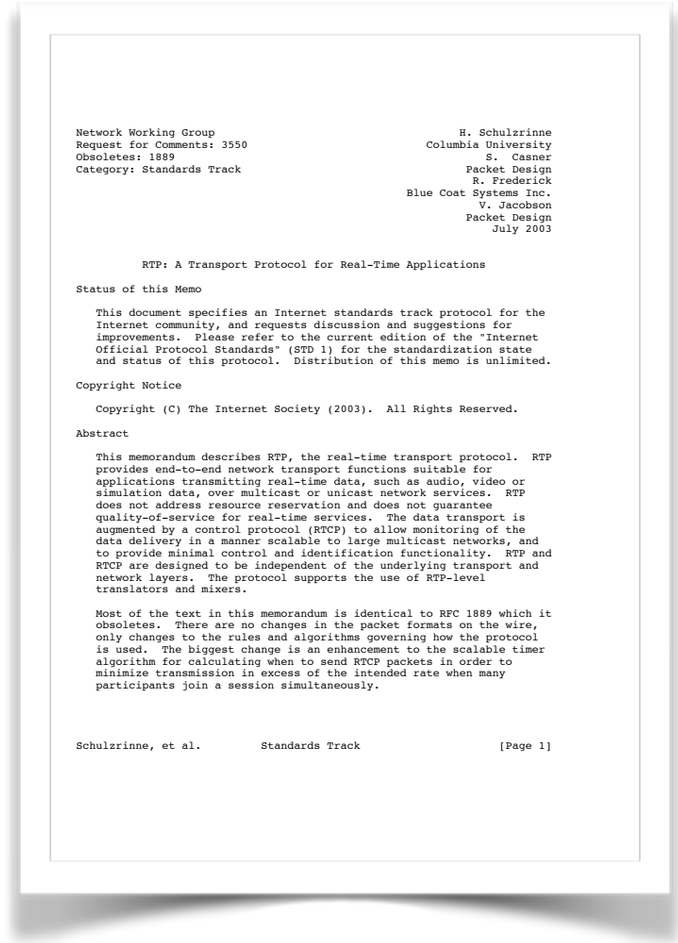
Colin Perkins

Real-time Transport Protocol Framework

- RTP: A Transport Protocol for Real-Time Applications
  - RFCs 3550 and 3551
  - Numerous associated payload format specifications
  - Numerous extensions for feedback, error correction, FEC, etc.

- A framework for real-time multimedia transport on the Internet – extremely widely deployed
  - Voice-over-IP
  - Video conferencing
  - Telepresence
  - WebRTC
  - 3GPP IMS and VoLTE

- Requires a separate signalling protocol to setup calls and negotiate media formats
  - SIP, H.323, RTSP, Jingle, WebRTC, …



Network Working Group
Request for Comments: 3550
Obsoletes: 1889
Category: Standards Track

H. Schulzrinne
Columbia University
S. Casner
Packet Design
R. Frederick
Blue Coat Systems Inc.
V. Jacobson
Packet Design
July 2003

RTP: A Transport Protocol for Real-Time Applications

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This memorandum describes RTP, the real-time transport protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.

Most of the text in this memorandum is identical to RFC 1889 which it obsoletes. There are no changes in the packet formats on the wire, only changes to the rules and algorithms governing how the protocol is used. The biggest change is an enhancement to the scalable timer algorithm for calculating when to send RTCP packets in order to minimize transmission in excess of the intended rate when many participants join a session simultaneously.

Schulzrinne, et al. Standards Track [Page 1]

How to Secure the RTP Framework?

- Core RTP specifications offer only limited security – how to evolve the protocol to be more secure?

- What recommendations should the IETF make concerning mandatory-to-implement security for the real-time transport protocol (RTP) framework?
  - What are the IETF policies in this area?
  - Why are they difficult to apply in the case of RTP?

IETF®

What are the IETF policies in this area?

- Danvers Doctrine
  32nd IETF meeting, 1995

  “IETF should standardise on the use of the best security available, regardless of national policies”

- RFC 1984
  Statement on Cryptographic Technology and the Internet

  “Encryption is not a secret technology monopolised by any one country” – strong encryption needed to protect privacy and secure commerce

- RFC 3365
  Strong Security Requirements for IETF Standard Protocols

  “MUST implement strong security in all protocols to provide for the all too frequent day when the protocol comes into widespread use in the global Internet” – must be implemented, not must be used

- RFC 7258
  Pervasive Monitoring is an Attack

  “Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible”

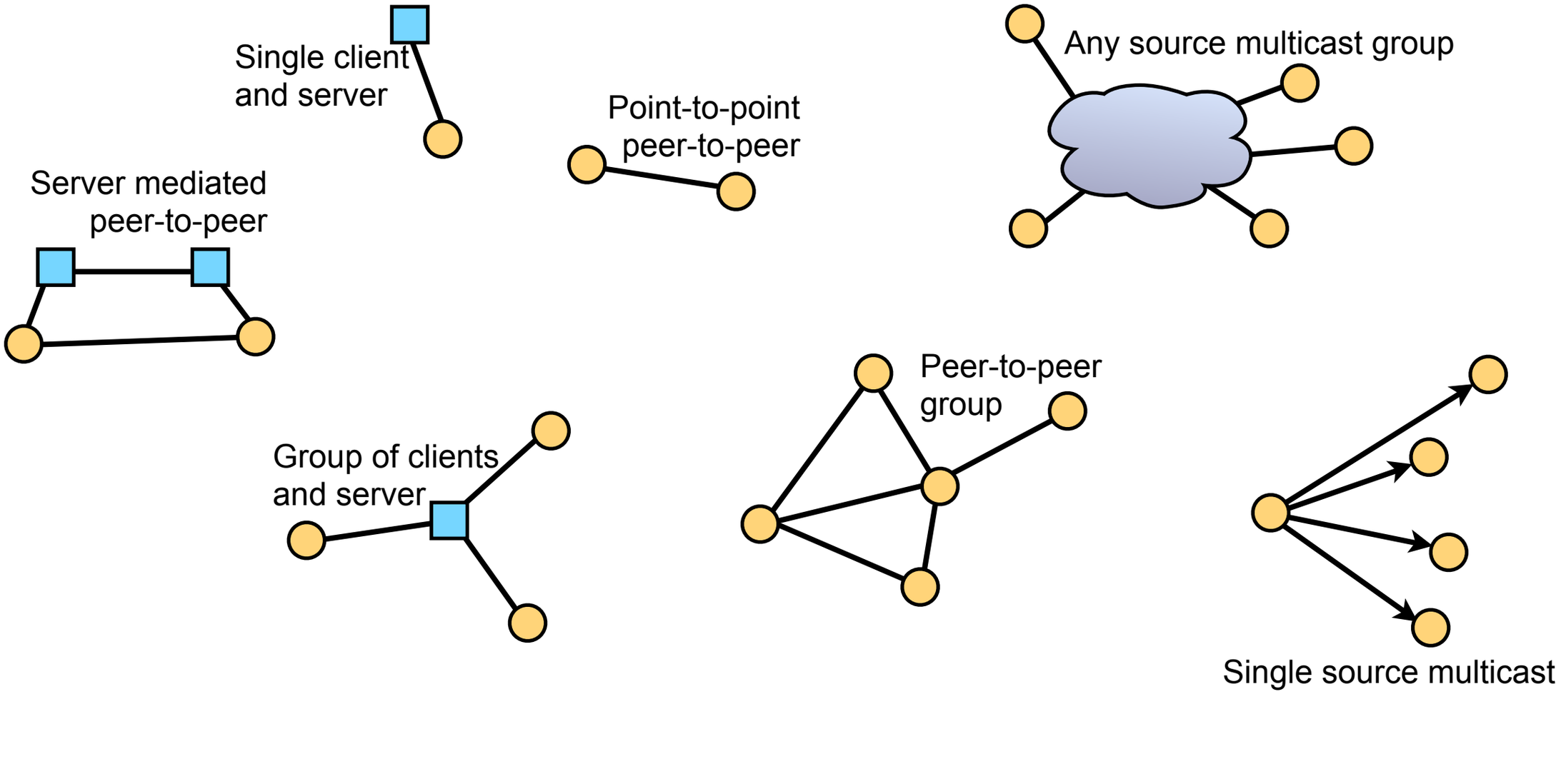
Strong, mandatory-to-implement, security is a requirement for IETF standard protocols

Why are these policies difficult for RTP?

- RTP is a framework, complicating design space:
  - Topologies
  - Application scenarios
  - Security requirements

Topologies

- RTP is inherently a group communication protocol
- Wide range of deployed application topologies



Application Scenarios (1)

- Fixed and mobile telephony
- Video conferencing and high-quality telepresence
- Group conferencing and telepresence, using centralised MCU
- Group conferencing using Mbone-style multicast
- Video streaming
- Internet TV – cable TV replacement using SSM
- Peer-to-peer audio – in-game audio
- TV production – interconnecting components in a TV studio
- Simulation – e.g., interconnecting parts of a flight simulator
- Streaming real-time sensor data – e.g., eVLBI

Application Scenarios (2)

- Complex design space – conflicting requirements:
  - Building blocks for real-time applications
  - Unicast *vs* small group *vs* large TV audience
  - Interactive *vs* non-interactive
  - Low bandwidth *vs* high bandwidth
  - Reliable *vs* non-reliable
  - Adaptive best effort *vs* managed service

Application Security Requirements

- Requirements vary across different applications:
  - Confidentiality
    - Who has access to media? For how long?
    - Complexity due to group membership changes
    - Trust in middle-boxes providing group conferencing service
  - Integrity protection
    - Middle-boxes required for many services, but trust issues
    - Many application require in-network media modification (mixing; advertisement insertion)
  - Source authentication
    - How is source identity asserted?
    - Is it necessary to authenticate individual members of a group, or is it sufficient to authenticate them as a valid member of the group?
  - Privacy
    - Network address or physical location of user may be sensitive
- Requirements can conflict with each other

Securing the RTP Protocol Framework

- RTP application and security requirements vary:
  - Securing TV distribution
  - Securing point-to-point telephony
  - Securing group videoconference
  - Etc.
- All share common media transport protocol: RTP

Building Blocks: Media Security

- Range of media security options:
  - Run RTP over a secure network layer:
    - IPSec – but security relationships often per-user, not per-host
  - Run RTP over a secure transport layer:
    - RTP over Datagram TLS or TLS – prevents header compression; no multicast support; needs trusted middlebox
  - Secure the protocol:
    - SRTP – headers unencrypted to allow header compression, leaking information; weak support for source authentication in groups; requires trusted middleboxes in some cases
  - Secure the media:
    - ISMACryp – protects payload integrity, but doesn't address privacy

- None suitable for all applications

Building Blocks: Secure Signalling

- Range of session establishment building blocks:
  - DTLS-SRTP – unicast
  - MIKEY – unicast or small group
  - SDP security descriptions – hop-by-hop security, expose key to middlebox
  - ZRTP – unicast
- None suitable for all applications

Mandatory-to-Implement Security for RTP

- Wide range of security building blocks – none work for all scenarios or topologies
- Conflicts with IETF policy on protocol security:
  - IETF requires mandatory-to-implement strong security for all protocols
  - But, no available mechanism works for all uses of RTP
  - Problematic for standardisation of RTP extensions
- Resolution: secure application scenarios, not the underlying protocol
  - Mandatory-to-implement security for RTP *when used for telephony*
  - Mandatory-to-implement security for RTP *when used for TV distribution*
  - RFC 7202 “Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security solution”

Conclusions

- IETF policy on secure protocols doesn't reflect use of framework protocols
  - Protocols are building blocks – usage scenarios can significantly impact how a protocol should be secured
  - May not be possible to devise mandatory-to-implement security that can work for all uses of framework – may need to be per-application domain
  - Challenge: are scalable security frameworks, that scale across application scenarios and topologies, feasible?

- Implications
  - Security architectures being developed for uses of RTP
  - IETF TAPS working group evolving transport to more general framework; issues encountered with RTP may see wider relevancy – policy will have to evolve