# RSVP Cryptographic Authentication

Fred Baker
Cisco

Mohit Talwar
Bob Lindell
USC/ISI

# Introduction

- Integrity and authentication
- Protection against replay attacks
- No confidentiality

# Approach

- Add an INTEGRITY object to an RSVP message
  - Flags [New]
  - Key identifier
  - One-time sequence number
  - Message digest (or other Integrity data)

# Key Management

- Key Identifier refers to an algorithm and the associated key
- Key and key identifier are simplex
- Key and key identifier are distributed out of band
  - Key identifier and key distributed between an outgoing router interface and all potential next hop receivers
- Key identifier has a defined lifetime
- Key switchover procedures account for uncertainty in clock synchrony between a sender and multiple receivers

# Initialization Handshake

- For protection against replay attacks
- Receiver sends challenge to sender
- Sender responds with challenge and current sequence number
- Does not assume clock synchrony
- Handshake may not be necessary in some operational settings

# Changes

- Key Identifier need only be unique per sender, not globally unique
- No-Handshake flag
- Key Management abstract interface
- Distinct Integrity Challenge and Response messages

# Competing design goals

- Small Integrity objects (Distribute keys out of band)
- Support auto configuration of keys (Distribute keys in band)
- Potential Solutions
  - Distribute keys in band (Large Integrity objects)
  - Extend handshake exchange to establish keys (and Policy objects?)
  - Transport reliability is a problem
  - New Ctypes for Challenge and Response messages

# Draft Status

- Still held back from the rest of the document set
- Complete except for a key distribution mechanism
- Should key distribution issues (e.g. auto configuration) be addressed in a separate draft?
- Can we reach consensus on the current draft?

# Status

- Reference implementation in ISI RSVP rel4.2a5 (Coming Soon)
- Current features not implemented
  - Key management abstract API
  - Management of Key lifetimes