RSVP Cryptographic Authentication

Fred Baker
Cisco

Mohit Talwar
Bob Lindell
USC/ISI

Introduction

- Hop-by-Hop (IPSEC is End-to-End)
- Integrity and authentication
- Protection against replay attacks
- No confidentiality

Approach

- Add an INTEGRITY object to an RSVP message
  - Key identifier
  - One-time sequence number
  - Message digest

Key Management

- Key Identifiers refer to an algorithm and the associated key(s)
- Key(s) and key identifiers are simplex
- Key(s) and key identifiers are distributed out of band
  - Key identifiers and key(s) distributed between an outgoing router interface and all potential next hop receivers
- Key identifiers have a defined lifetime
- Key switchover procedures account for uncertainty in clock synchrony between a sender and multiple receivers

Sequence Number Generation

- One-time for the life of a key identifier
- Monotonically increasing modulo 2^{64}
- Requires stable (recoverable) storage
  - Message counter
  - Pseudo timestamp based on RTC hardware
  - Pseudo timestamp based on NTP

Key Identifier Generation

- Should be unique for any receiver
- Partitioned generation
  - Key identifiers are a function of source IP address, LIH, and key number
- Random generation
  - Improved protection against non-compliant implementations

Initialization Handshake

- 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

Message Processing Rules

- Sender
  - Choose key identifier
  - Generate sequence number
  - Generate message digest
- Receiver
  - Check message digest
    - Use multiple keys if necessary
  - Reject message if no match with digest
  - Check sequence number to prevent replay
    - Out of order message delivery tolerance

Out of Order Message Processing

Accepted message list: $[N_i, N_{i+1}, N_{i+3}, ..., N_{i+19}]$

Receive $N_{i-2} \Longrightarrow$ Reject

Receive $N_{i+3} \Longrightarrow$ Reject

Receive $N_{i+2} \Longrightarrow$ Accept

Accepted message list: $[N_{i+1}, N_{i+2}, N_{i+3}, ..., N_{i+19}]$

Receive $N_{i+30} \longrightarrow$ Accept

Accepted message list: $[N_{i+2}, N_{i+3}, ..., N_{i+19}, N_{i+30}]$

Status

- Reference implementation in ISI RSVP rel4.2a4
- Current features not implemented
  - Handshake
  - Out of order message delivery tolerance
  - Key management