RSVP Cryptographic Authentication

Fred Baker

Cisco Systems

Problem Being Solved

- RSVP Enables Arbitrary Consumption of Network Resources
- Hackers Like to Consume Resources
- Need to Know That RSVP Messages Are From Who They Appear to Be From
- Need to Avoid Common Pitfalls
  - Password Snooping
  - Replay Attacks
  - Computational Intensity

History of Draft Text

- Proposed to OSPF WG by Christian Huitma
- OSPF Authentication Draft: Baker and Atkinson
  - Prototyped by Jeff Honig/Cornell gated
  - Implemented in Cisco 11.0 Release
  - Incorporated into base standard
- RIP V2 Authentication Draft: Baker and Atkinson
  - Prototyped by Jeff Honig/Cornell gated
  - Recently approved with minor updates
- Proposed to RSVP Working Group
  - Initial Draft 3/95
  - Update largely an edit by Bob Braden

Key Assumptions

- External Key Management
- Keyed MD5 Effectiveness (RFC 1321)
  - RSVP Checksum Not Needed
- Key Attributes
  - Content
  - Algorithm
  - Lifetime

Object Proposed

Length = 28	Type = 1	
Key Identifier		
Sequence Number		
Keyed Message Digest		

Sequence Number

- Addresses Replay Attacks
- Not monotonically Increasing
  - Burst of messages might pass each other…
- Rather, Non-decreasing
  - Replay attack recognized as decreasing sequence number

Message Generation

- Construct Message
- Add RFC 1321 Trailer
- Write Secret Into Integrity Object
- Calculate Message Digest
- Write Digest Over Secret
- Remove Trailer
- Send Message

RFC 1321 Trailer

Zero or more bytes of 10000000…
Message Length Most Significant Word
Message Length Least Significant Word

Message Reception

- Receive Message
- Add RFC 1321 Trailer
- Save Digest From Security Object
- Overwrite Digest With Secret
- Calculate Message Digest
- Compare Digests
- If Identical AND Sequence Number ≥ Last Received, Accept

Key Management

- Every Key Has
  - Identifier
  - Key Value
  - Algorithm
  - Start of Use
  - End of Use
- Change Keys When New Key Lifetime Starts
  - Send With New Key
  - Receive With Any Active Key

Configuration

- Neighboring Router Not RSVP Router
  - Key Configured for Interface
  - Think Multicast…
- Neighboring Router Not RSVP Router
  - Received Message Key Selected by Source Address

Pathological Cases

- What If Key Expires With No New Key Installed?
  - Keep Using the Old Key
- What If Neighbor Is Doing That?
  - While Key Is Valid, Continue to Accept Messages With Old Key
  - While Key Is Valid, Send With BOTH Keys