RSVP Cryptographic Integrity Object

Fred Baker

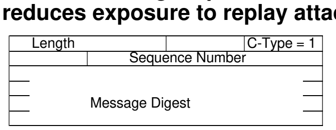
Cisco Systems

Observations

- We depend on transitive relations in
  - Routing
  - Policy
  - Authentication
- RFC 1323 MD5 algorithm already implemented in SNMPv2, OSPF, etc.
- Need authentication, not privacy

Object format

- MD5, potential for SHA or other algorithms
- Untransmitted shared secret
- Non-decreasing sequence number reduces exposure to replay attacks



Transmission algorithm:

- Build message with shared secret in object
- Pad according to RFC 1323 MD5 algorithm
  - one bit of 1
  - some number of zeroes
  - 64 bit length field
  - resulting mod (message length, 512 bits) == 0
- Calculate digest
- Overwrite secret with digest
- Remove trailer

Reception algorithm

- Verify
  - message size, etc. as usual
  - sequence number ≥ last received
  - key number ==> one of the active keys
- Pad according to MD5 algorithm
- Save digest in hip pocket
- Overwrite digest with secret
- Calculate digest
- If calculated digest == received digest, consider valid

Key management

- Shared secret by neighbor or interface
  - multicast ==> per interface
  - tunneled neighbors ==> per neighbor
- When more than one active key,
  - encode with most recently started,
  - decode with any valid key
- Keying algorithm attribute of key used
- Key switchover requires some care

Performance Considerations

- **Anyone who told you MD5 was fast was mistaken- fast is not the point**
- **Little need for UDP/RSVP checksums in presence of MD5 Checksum**

129_025/c5 7