Distributing integrity keys used for routing and signaling protocols

Brian Weis

Sheela Rowles

Background

- Many routing & signaling protocols are group applications
- These protocols usually define an integrity option
  - A simple MAC based on MD5 and/or SHA1
- Often these protocols defined their integrity option before IPsec was finalized
  - And they don't seem to be inclined to change their protocol definitions
- This work explores the possibility of providing automated key management for those protocols
  - Keys are manually configured

Possible Protocols

- Unicast routing protocols (OSPF, RIP, IS-IS) are possibilities
  - But obtaining keys from a key server used to protect routing packets is problematic if routing isn't available!
  - A siginificant amount of group key management protocol work is necessary to address unicast routing protocols, so these are not addressed at this time
- Signaling protocols (RSVP, NLS) do not have the routing limitation

RSVP

- It was recognized that Resource ReSerVation Protocol (RSVP) sometimes requires the use of a group trust model (e.g., within a provider network)
  - RSVP messages sometimes carry the source and destination addresses of the hosts seeking to reserve bandwidth in the network
  - RSVP devices along the routed path receive, inspect, modify, and forward the RSVP message
  - The next RSVP device on the routed path may not be the next hop, which may make pair-wise RSVP keys unsuitable
- See draft-ietf-tsvwg-rsvp-security-groupkeying-00.txt for details

Initial proposed solution

- RFC 3547 (GDOI) is a group key management protocol
  - Distributes ESP SA attributes and keys to a group of devices for the purpose of encrypting IP multicast packets.
  - Can be used to distribute other types of group policy and keys
- draft-weis-gdoi-for-rsvp-00 was proposed to distribute RSVP INTEGRITY Object policy and keys
- At my IETF 70 MSEC WG presentation, it was observed that many routing/signaling protocols require a simple integrity key
  - It was recommended that this draft be made more general
  - Adding routing protocols seems premature, so we looked for another candidate protocol

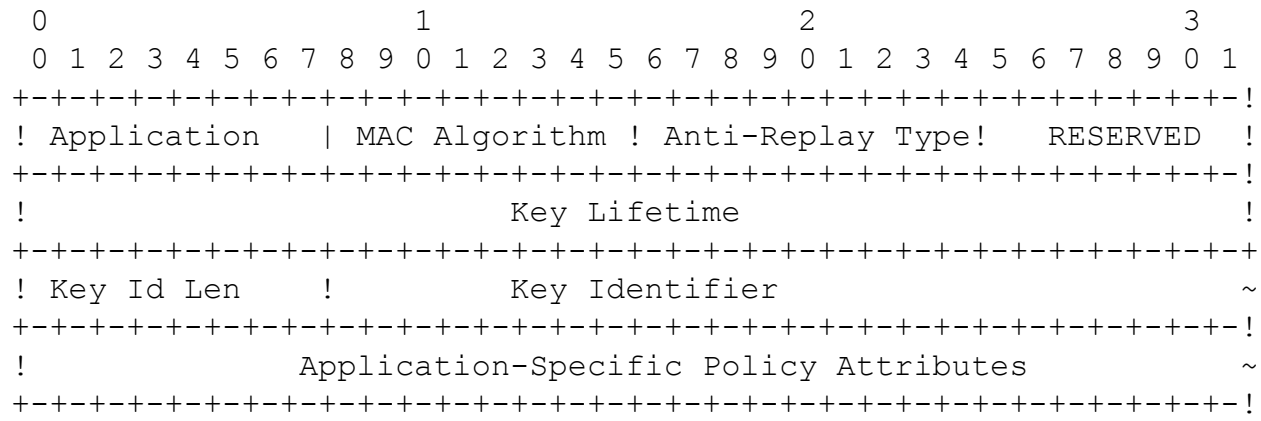
NLS

- draft-shore-nls-tl-05.txt is one another signaling protocol
  - Network-Layer Signaling: Transport Layer
  - Implemented by Packet Cable for NAT Traversal
  - Intended to be published as an Informational RFC

What needs to be distributed?

- An integrity key
- MAC algorithm
- Other policy info, such as
  - Lifetime
  - Replay protection method

Proposed GDOI SA TEK



- Application type (e.g., RSVP, NLS)
- MAC Algorithm (e.g., HMAC-SHA)
- Anti-Replay type (counter or time)
- Key lifetime (distributed in seconds)
- Other Policy Attributes

Application Type: RSVP

- According to RFC 2747:
  - MAC Algorithm: HMAC-MD5 (required) HMAC-SHA1 (recommended)
  - Anti-replay types: counter & time
  - Key lifetime used
  - Optional attributes
    - KeyStartValid (start time)
- The MAC key is distributed in a GDOI KD payload

Application Type: NLS

- According to the I-D:
  - MAC Algorithm: HMAC-SHA1 (default)
  - Anti-replay types: counter
  - Key lifetime set to zero (indicating no end time)
  - Optional attributes
    - List of Application Group Identifiers (AGIDs) describing what NLS applications in which the group member is authorized to participate
- A MAC key for each AGID is distributed in a GDOI KD payload

Existing GDOI features used

- GDOI registration provides authentication & authorization of group members
- GDOI rekey protocol provides dynamic key updates
- LKH group management algorithm for revoking group members

Next steps

- Is there support for defining the proposed integrity-only GDOI protocol extensions in the MSEC WG?
  - Definitions for RSVP and NLS included now
  - Definitions for unicast routing protocols can be added in the future