A Group Security Model for RSVP Message Authentication

Brian Weis
Outline

• Resource ReSerVation Protocol (RSVP) Overview
  – Architecture
  – Integrity Protection
  – Manual Keying Issues

• RSVP Group Trust Model
  – draft-behringer-tsvwg-rsvp-security-groupkeying-01

• GDOI Extensions to support Group Secured RSVP
  – draft-weis-gdoi-for-rsvp-00
RSVP Overview

- RSVP provides setup of resource reservations for multicast or unicast data flows.
- Receivers of the data flow request a specific QoS, which is relayed hop by hop toward the data flow source.
  - Each receiving hop intercepts & possibly alters the RSVP packet before forwarding it.
  - RSVP Source and Destination may be in different security domains, where the domains co-operate.
RSVP Authentication
Overview

• RFC 2474 (updated by RFC 3097) specifies an INTEGRITY Object for RSVP, which included the following protection
  – Message integrity
    • HMAC-MD5 or HMAC-SHA result, created and verified with a shared key
  – Replay protection
    • Sequence Number (Counter or Time based)

• RSVP integrity keys are commonly configured manually (although other methods are allowed)
Pair-wise Manual Keying

• A pair-wise key can be used when an RSVP router knows which RSVP peer will be the RSVP next-hop. E.g., when
  – Keys are bound to a specific interface
  – The next hop router is known to be the RSVP next-hop router
  – Particularly appropriate when used between trust domains, where paths between trust domains is unambiguous.
Pair-wise Manual Keying

Issues

• Manual keying within a single trust domain (e.g., provider) is not optimal
  – The presence of multiple paths through the network makes pair-wise keys problematic
Group Manual Keying Issues

• Within a single trust domain a single group key can be manually shared
  – But manually shared group keys are difficult to manage, suffer from overuse, etc.
Intra-domain trust model

• Within a single trust domain, RSVP routers are jointly managing QoS policy, and share an implicit trust
  – RSVP speakers trust other RSVP speakers to correctly perform RSVP semantics
  – An RSVP router does not know which other RSVP speakers touch a packet, except those with which it peers

• An RSVP router explicitly trusts its peers, insomuch that it exchanges INTEGRITY objects.
  – As previously shown, in some configurations a group key between a set of RSVP routers is used, although predicting which RSVP routers comprise a group may be problematic
Dynamic Group Key Management

• Dynamic group key management of the RSVP integrity keys can ease both the configuration and quality the group keys.

• Dynamic group key management can provide group management services (e.g., de-authorize an RSVP router by removing it from the group).
GDOI Extensions for RSVP

- draft-weis-gdoi-for-rsvp-00 describes updates that allow GDOI to distribute RSVP integrity keys
  - SA TEK specific to RSVP
  - Define how the keys are passed in the KD payload
SA TEK

- Key identifier uniquely identifies a key
- MAC Algorithm (HMAC-SHA or HMAC-MD5)
- Sequence number type (counter or time)
- Key lifetime
- Optional Attributes
  - KeyStartValid (Timestamp for when to begin using the key)
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

• We will work towards having draft-behringer-.tsvwg-rsvp-security-groupkeying-01 is accepted by the TSVWG WG as a working group draft
• If this happens, we’d like draft-weis-gdoi-for-rsvp-00 to be considered as a MSEC WG work item
  – Implementations of the TSVWG WG draft needs the GDOI extensions described in the MSEC WG draft
• In the meantime, we’d like feedback on whether there is support for doing such work in the MSEC WG.