Analysis of RSVP-TE Security According to KARP Design Guide

draft-mahesh-karp-rsvp-te-analysis-01.txt

M. Jethanandani
Ciena Corporation
D. Zhang
Huawei Technologies co., LTD.

Existing Security of RSVP-TE (1)

- RSVP Security Properties [RFC4230] indicates the unfeasibility of using IPSec to secure RSVP signaling messages.
- RSVP Cryptographic Authentication [RFC2747] describes the format and use of RSVP's INTEGRITY objects to provide hop-by-hop integrity and authentication of RSVP messages.
- RSVP-TE: Extensions to RSVP for LSP Tunnels [RFC3209] is an extension of the RSVP protocol to establish Multi- Protocol Label Switching (MPLS) Label Switch Paths (LSPs).
- Currently, there is no security approach specified for RSVP-TE particularly. However, the security mechanisms for RSVP RSVP Cryptographic Authentication [RFC2747] can be taken advantage of to provide the security protection for the RSVP-TE message transportation.

Existing Security of RSVP-TE (2)

- There is a requirement that RSVP-TE headers and payload be authenticated. There is no requirement that they be encrypted and that work is outside the scope of KARP WG. RSVP Cryptographic Authentication [RFC2747] outlines the use HMAC-MD5.
- RSVP uses 64 bit monotonically increasing sequence numbers to prevent against replay attacks. To address the issue of out-of-order message delivery, the solution allows administrators to specify a sequence number window corresponding to the worst case reordering behavior.

Existing Security of RSVP-TE (3)

- The solution provides three approaches to generate unique monotonically increasing sequence numbers across a failure or a restart. The solutions include:
  - Maintaining sequence numbers in stable memory
  - Introducing the data from a local time clock into the generation of sequence numbers after a restart
  - Introducing the timing information from a Network Recovered Clock into the generation of sequence numbers after a restart.
- A handshake is defined for a receiver to get the latest value of a sequence number. Therefore, this solution is effective in addressing the issues caused by the rollback of sequence numbers across a system restart or failure.

Gap Analysis for RSVP-TE

- In order to fulfill the requirement of supporting strong algorithms, at least the support of SHA-2 needs to be provided.
- Three approaches to generating unique monotonically increasing sequence numbers across a failure and restart are introduced, but no approach is mandated.
- However, when a router uses the approach to generating sequence numbers with the time information from NTP, an attacker may try to deceive the router to generate a sequence number which is less than the sequence numbers it used to have, by sending replayed or foiled NTP information.

Other Security Work Undergoing

- **Cryptographic Agility for the RSVP INTEGRITY Object (draft-turner-rsvp-auth-update)**
  - **This work intends to address the issues we mentioned in the gap analysis**
  - **This work also tries to describe how RSVP-TE cooperates with key table**

- Questions?