Where to Perform Authentication for Reliable Multicast?

Miriam Kadansky
Sun Microsystems Labs

Background

Architecture draft specifies use of IPSec for authentication in multicast sessions.

Drawback: unsuitable for several **reliable** multicast protocols (and requires full deployment of IPSec).

Repair Nodes in Reliable Multicast

- SRM, TRAM, RMTP-II, etc., use various nodes for repair
- Repair nodes may not be determined in advance
- Problem: IPSec information is stripped below transport. Any retransmission performed by the transport gets a new IPSec header.

Possible Workarounds

1. Use group authentication since source authentication is not possible

2. Receivers have repair node's key (pre-configured or obtained dynamically)

3. Receivers don't authenticate repairs (possible?)

4. All repairs must come from the sender

Authentication above the Transport?

Issues:

- If transport passes packet up to authentication layer, and it fails, what happens?
- could transport be notified by authentication layer to obtain a repair for a bogus packet?
- how would the transport back out the bad packet?
- what about transport control packets?

Performing authentication above the transport requires tight interaction

Recommended Solution for RM

- Support authentication at the transport layer
  - must authenticate before any other transport operations
  - otherwise, bogus packet may preempt authentic packet (DOS attack)
- repair nodes can now retain received packets with **original** signatures for retransmission
- Side benefit - does not require full IPSec deployment