Securing PIM-SM Link-Local Messages

J.W. Atwood
Salekul Islam
Concordia University

draft-atwood-pim-sm-linklocal-01

Problem Statement

- PIM-SM draft says
  - Recommend AH
  - Assume manual keying, but allow automatic
  - If IPsec, MUST authenticate all
  - Anti-replay SHOULD be enabled
- AH says
  - SHOULD NOT offer anti-replay when manually keyed

cont

- IPsec says
  - Security Policy Database (SPD) cannot represent a creation policy for a multicast SA
  - Therefore, only manually-configured SAD entries are possible
- Apparent conclusion
  - We should not activate anti-replay for PIM Link-local messages
- Actual conclusion
  - We can, it’s just harder…

Per–interface or per–sender?

- PIM–SM says
  - Per–interface may be useful
- IPsec says
  - No (longer) need to support per–interface
- AH says
  - Use SPI + destination + source for SSM
  - Use SPI + destination for ASM

Who talks to whom?

- Link-local messages go from one router to all its peer routers
- Since all routers use ALL_PIM_ROUTERS, it looks like an ASM group
- In fact, this is a collection of SSM groups
- Therefore
  - All the counsel against anti-replay for multi-sender multicast groups does not apply
  - Link-local SA SHOULD be established as an SSM group

Choices

- Declare that ALL_PIM_ROUTERS operates as an SSM group when IPsec is enabled
  - This may be hard, because ALL_PIM_ROUTERS is used for BSR communication
- Define LINK_LOCAL_PIM_ROUTERS or SECURE_PIM_ROUTERS to be in the SSM address range
  - But, we will need to secure BSR communication as well

Manual Key Configuration

- Number of peers will be small
- AH says
  - Anti-replay SHOULD NOT be provided if SAs are manually keyed
- Choices
  - Override AH (RFC 4302)
  - Define a negotiation protocol to ensure key generation and SA refresh on counter overflow

Counter Overflow

- If Extended Sequence Number is specified, 2^{64} control packets can be sent
- This may justify overriding the AH prohibition.
- Otherwise, we are prepared to work on defining the necessary negotiation protocol

Validation

- This proposal was formally validated, as part of the Master’s Thesis of Salekul Islam, using PROMELA and the SPIN tool.

- Salekul Islam and J. William Atwood, "Security Issues in PIM-SM Link-local Messages", Proceedings of IEEE LCN 2004, Tampa, FL, 2004 November 16--18, pp. 402--403.

Contact Information

- PPT/PDF of these slides are at

  www.cse.concordia.ca/~bill/internet-drafts/IETF66-LinkLocal-01.ppt or IETF66-LinkLocal-01.pdf

- Email addresses
  - bill@cse.concordia.ca
  - salek_is@cse.concordia.ca