Multicast Support in IPsec

Russ Housley

10 March 2005

Background

- The MSEC WG coordinated with the IPsec WG to ensure that ESPv3 and AHv3 could accommodate multicast
- RFC 2401bis specifies the framework for ESP and AH as well as other components of the IPsec architecture
- RFC 2401bis, ESPv3, and AHv3 have completed IETF Last Call

Multicast Security Architecture

- Changes to ESPv3 and AHv3 are not sufficient
- RFC 2401bis (or an update to it) needs to reflect the multicast security architecture
  - Current SPD structure does not support multicast
  - Multicast SAs need to use a Group SPD (GSPD) as defined in RFC 3740
  - Current SAD structure only supports multicast when manually configured

Group SPD

- GSPD entries require a different structure
  - Symmetric relationship used for local and remote addresses in unicast SAs is not appropriate for multicast
  - Outbound traffic directed to a multicast address will not have a companion inbound SA with the multicast address as the source

SAD

- SAD can support multicast SAs, if manually configured
- Outbound multicast SA has the same structure as unicast SA
  - source = sender; destination = multicast address
- Inbound multicast SA must be configured with the source address of each peer authorized to transmit on the multicast SA
  - SPI value for a multicast SA is provided by a multicast group controller, not by the receiver
  - SAD structure already accommodates multiple IP source addresses
  - But, do not currently have an automated way to create a multicast SAD entry

Way Forward

- Let RFC 2401bis proceed
  - Publish as Proposed Standard
  - Close IPsec WG
- MSEC WG develop an update to address the multicast short comings

Questions?