draft-ietf-msec-ipsec-extensions-02

George Gross

Brian Weis

Dragon Ignjatic

Overview

- Changes from -01 to -02
- Next Steps

Composite Groups & Terminology Changes

- Composite groups moved to a separate draft, destined for Experimental state
- Terminology changes
  - SPD to Group Security Policy Database (GSPD), which matches RFC 3740 terminology
  - GKMP to GKM Protocol, which matches RFC 4046 terminology. It also avoids confusion with RFC 2094

UDP Encapsulation Requirement of ESP

- Added a new requirement:
  - This attribute declares that the UDP encapsulation of IPsec ESP packets [RFC 3948] will be used as part of an ESP SA.
  - Needed in the case of multiple sources behind the same NAT

New GSPD statements

- Registration
  - To facilitate dynamic group keying, the outbound GSPD MUST implement a policy action capability that triggers a GKM protocol registration exchange (as per [RFC4301] section 5.1).
- De-registration
  - The IPsec subsystem MAY provide GSPD policy mechanisms (e.g. trigger on detection of IGMP/MLD leave group exchange) that automatically initiate a GKM protocol de-registration exchange.

Proposed -03 change

- Current text says:

  "This specification requires that a GKM/IPsec implementation MUST support at least two concurrent IPsec SA per Group Speaker and this re-key rollover continuity algorithm."

- No change in -02, but after further discussion propose changing the requirement to a "qualified SHOULD" and state when it is reasonable to not support re-keying.
  - E.g., short-lived groups do not need re-keying

Next Steps

- Publish -03 with small changes within a month of this meeting.
  - ESP over UDP encapsulation in the NAT section
  - MUST support 2 SAs + rekey to SHOULD with qualifiers
- Send -03 to IPsec mailing list
- Publish -04 with any feedback, and ask for WG last call.